Troubleshooting ExpressWay & Mobile Remote Access

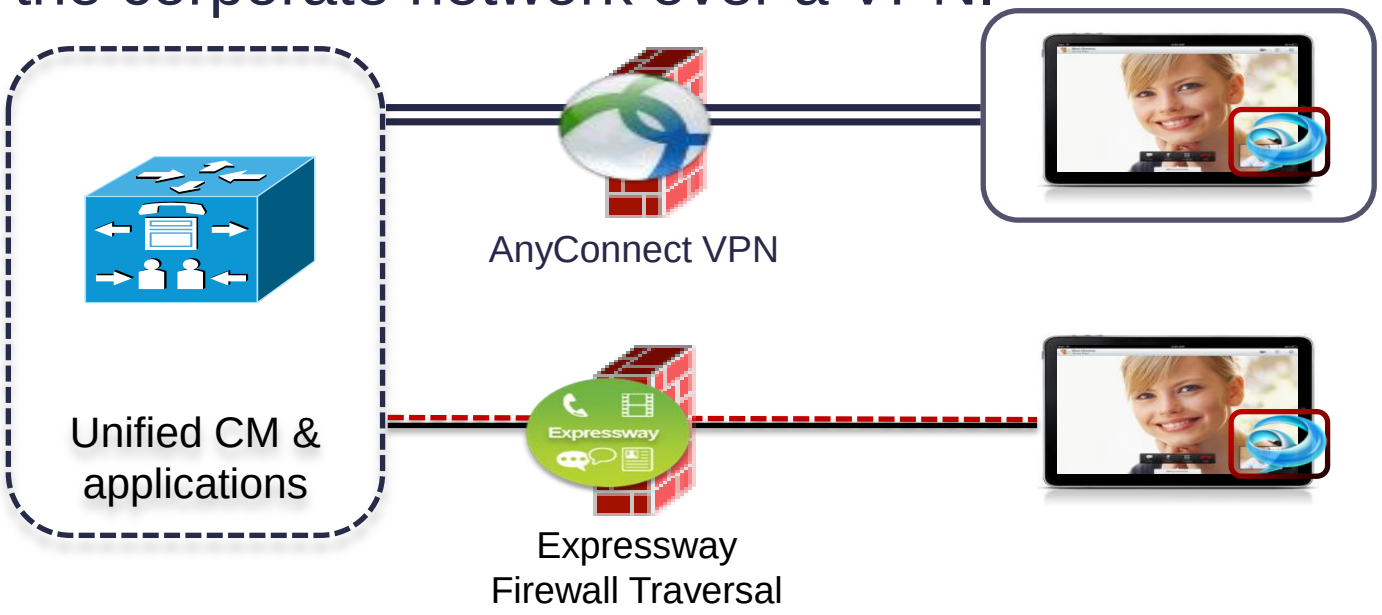
Michael Huang
Customer Support Engineer - China TAC Collaboration

Agenda

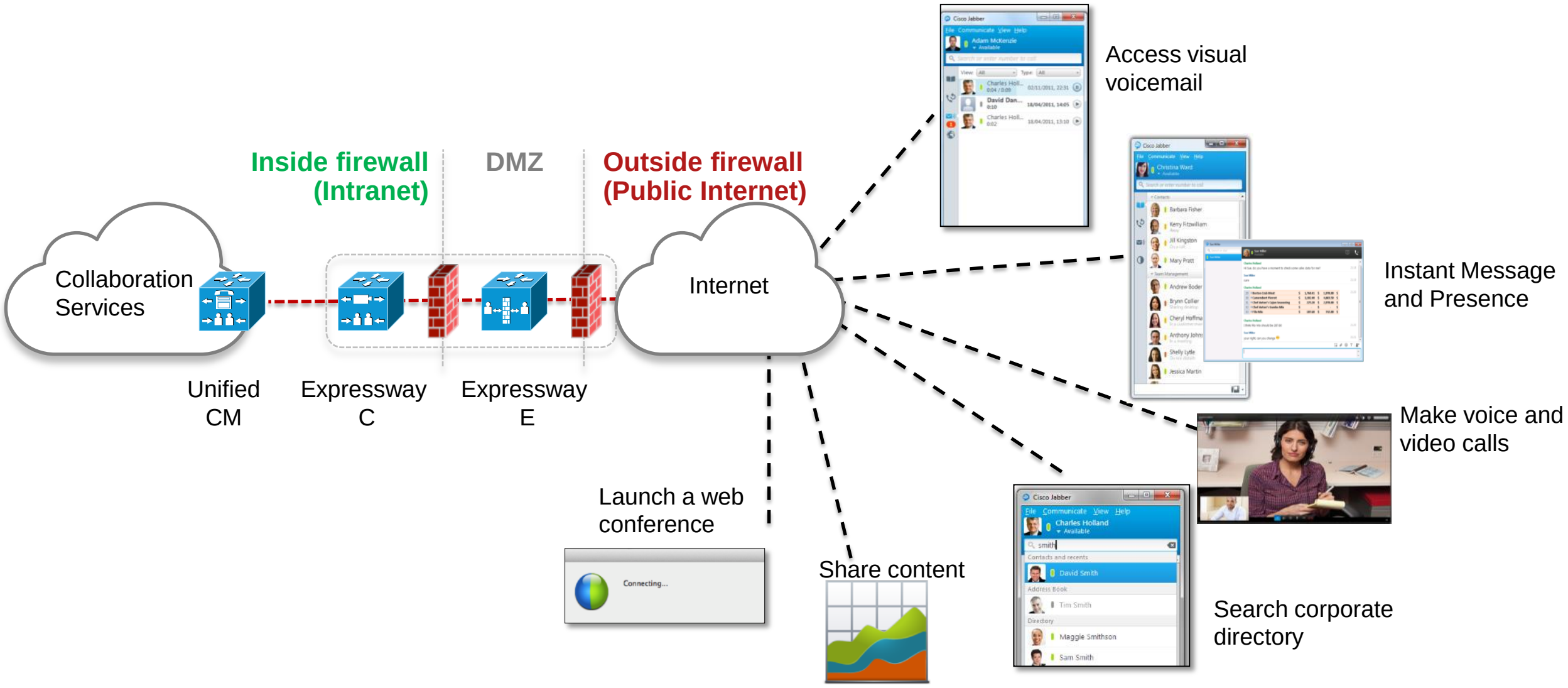
- Overview, ExpressWay and Mobile Remote Access
- ExpressWay Configuration
  - Firewall Settings
  - Certificate Requirements
  - Traversal Zone setup
  - UC server discovery
  - Domain and DNS
- ExpressWay serviceability
- Jabber registration and call walk through

What is ‘Mobile and Remote Access’ feature?

- Mobile and Remote Access
  The mobile and remote access solution supports a hybrid on-premise and cloud-based service model, providing a consistent experience inside and outside the enterprise.
  It provides a secure connection for Jabber application traffic without having to connect to the corporate network over a VPN.



What can a Jabber client do with Expressway?



Software Requirements

- CUCM 9.1(2)SU1 or above
- CUP 9.1(1) or above
- ExpressWay/VCS X8.1.1
- Jabber 9.7 (windows)

ExpressWay Configuration

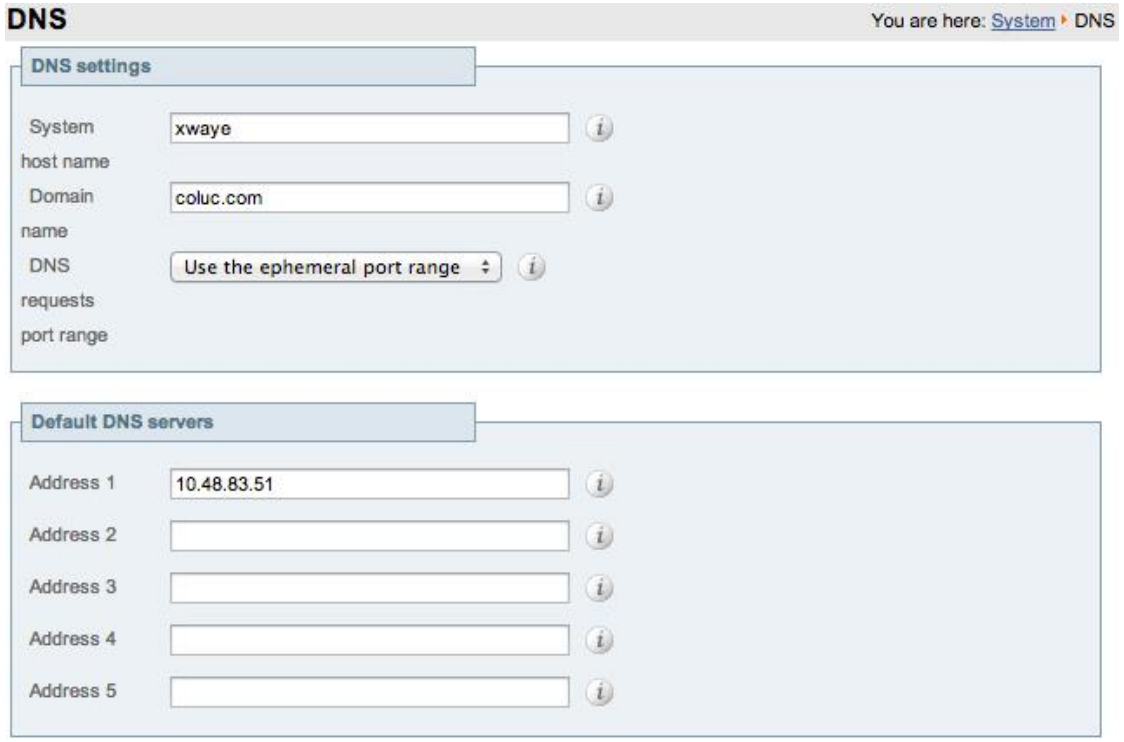
ExpressWay Configuration
Main configuration steps

1. System configuration
2. Firewall configuration
3. Certificate configuration and deployment
4. Traversal zone configuration
5. UC server discovery
6. DNS and domain configuration/deployment

Configuration System configuration

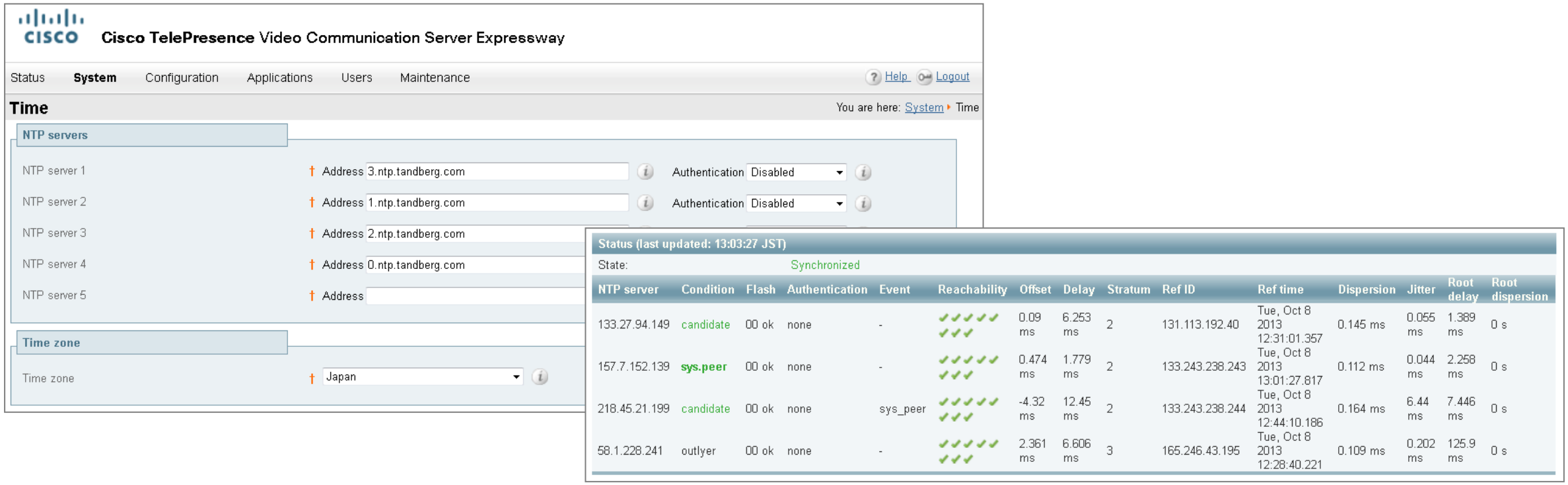
- System name and domain must be set for each server
- Each server must have proper DNS configuration

> System > DNS



Configuration System configuration

- Each system must be synched with NTP server > System > Time



Configuration System Configuration

- If NTP is not configured and synchronized on ExpressWay-C and ExpressWay-E Jabber Telephony registration to CUCM will not succeed.
- Security mechanism based on SIP SERVICE messages.

1. Expressway-E time-stamps a SERVICE message
2. Expressway-E sends the SERVICE message to Expressway-C
3. Expressway-C verifies the SERVICE is received within 60 secs error margin

Configuration System Configuration

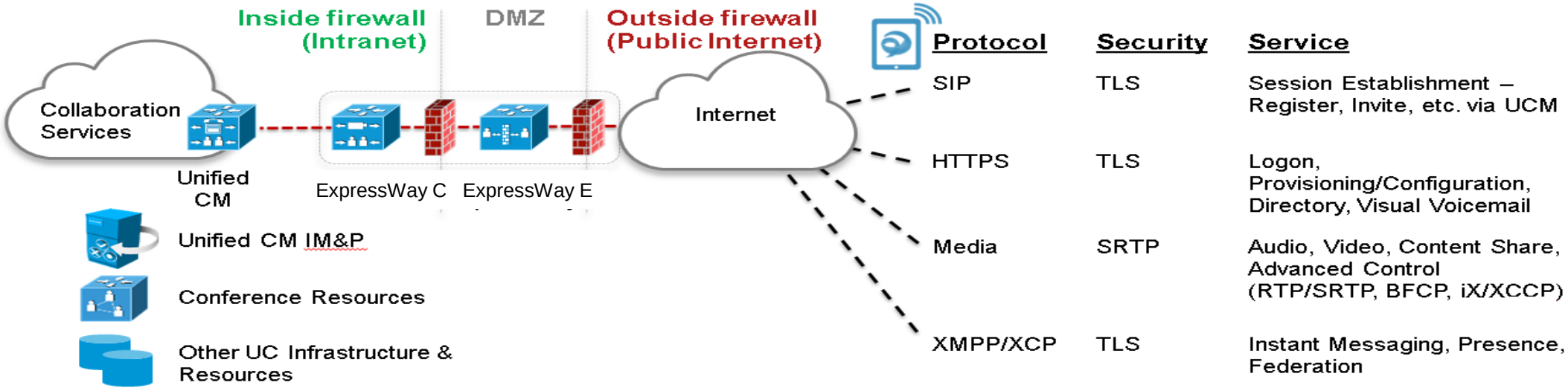
- Enable Mobile and Remote Access
  Configuration > Unified Communications > Configuration

- Check the Administrator guide for more help on system configuration topics

Firewall Configuration

Firewall Configuration

- What traffic does the firewall need to pass?
  - ✓ HTTPS proxy for secure provisioning of endpoints
  - ✓ SIP/TLS, RTP/SRTP for audio/video media
  - ✓ XCP/XMPP for IM&P for Jabber
  - ✓ Visual Voicemail (REST/HTTPS)
  - ✓ Traversal Connection between ExpressWay C and E



Firewall Configuration
To which ports does this translate?

- Port usage: ExpressWay C to Expressway E

		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
IP Ports	XMPP (IM and Presence)	TCP **Ue** 30000 to 35999 *	TCP 7400
	SSH (HTTP/S tunnels)	TCP **Ue** 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & **TLS_A** 25000 to 29999	TCP & **TLS_B** 7001
	SIP media	UDP **Y_C** 36000 to 59999 **	UDP **Y_E** 36000 to 59999 **

TCP & **TLS_A** = Configurable TCP Outbound ports range

TCP & **TLS_B** = Configurable traversal port for traversal link between Control and Expressway (i.e. 7001, 7002, etc.)

Ue = Configurable TCP ephemeral port range

Y_C = Configurable traversal media ports range (on Control/C)

Y_E = Configurable traversal media ports range (on Expressway/E)

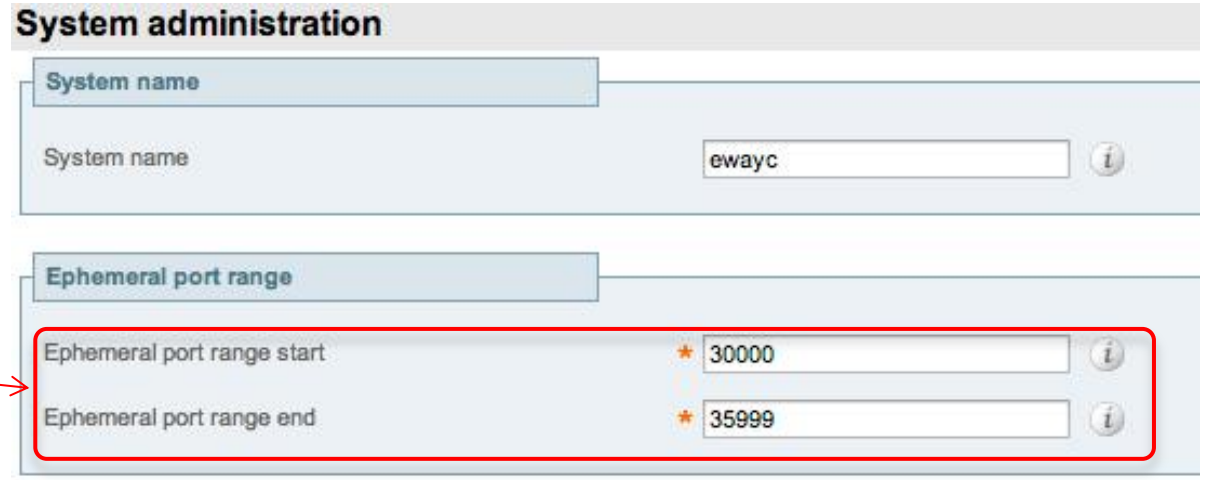
* Default ephemeral ports range (X8.1) for is 30000 – 35999 which configurable

** Default media ports range (X8.1) is 36000 – 59999 which configurable

Firewall Configuration
Where to configure these ports?

- ExpressWay C > System > Administration

		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
	XMPP (IM and Presence)	TCP **Ue** 30000 to 35999 *	TCP 7400
	SSH (HTTP/S tunnels)	TCP **Ue** 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & **TLS_A** 25000 to 29999	TCP & **TLS_B** 7001
	SIP media	UDP **Y_C** 36000 to 59999 **	UDP **Y_E** 36000 to 59999 **

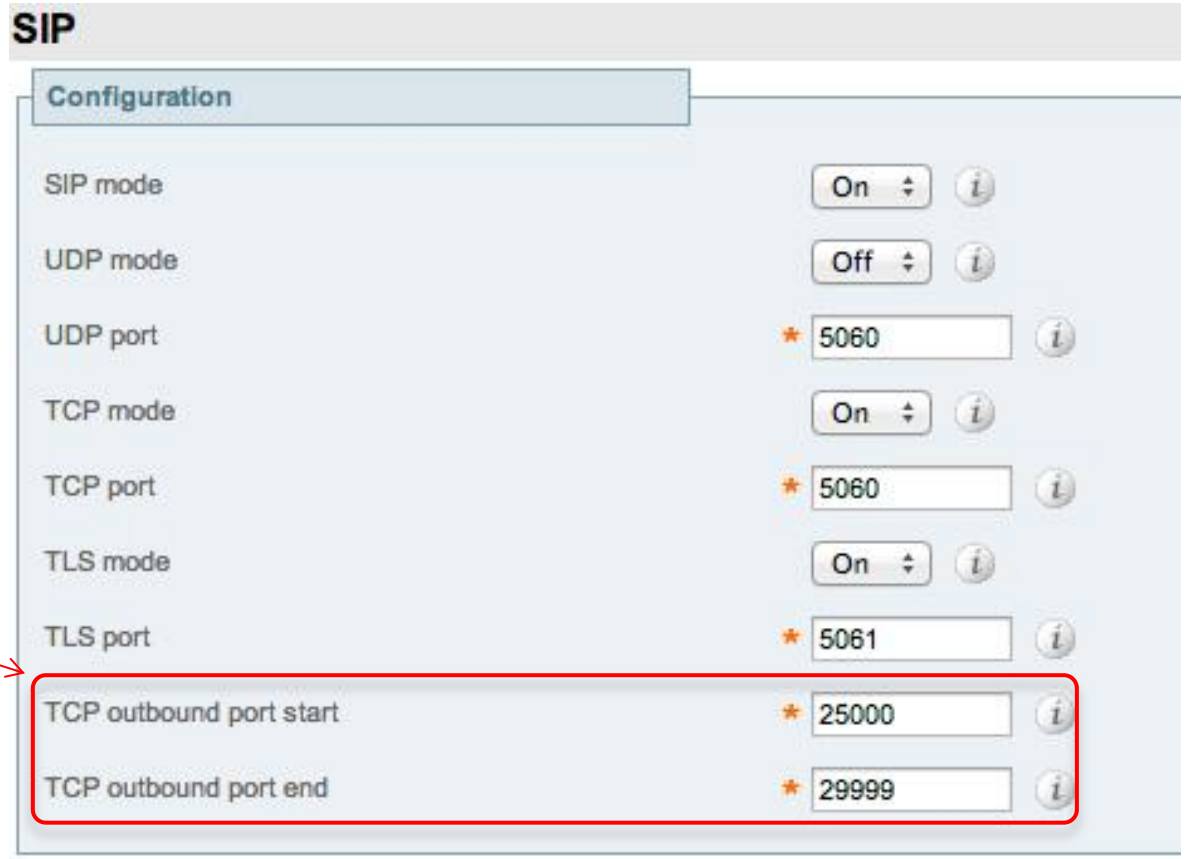


Firewall Configuration
Where to configure these ports?

- ExpressWay C

		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
	XMPP (IM and Presence)	TCP 7400	TCP **Ue** 30000 to 35999 *
	SSH (HTTP/S tunnels)	TCP **Ue** 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & **TLS_A** 25000 to 29999	TCP & **TLS_B** 7001
	SIP media	UDP **Y_C** 36000 to 59999 **	UDP **Y_E** 36000 to 59999 **

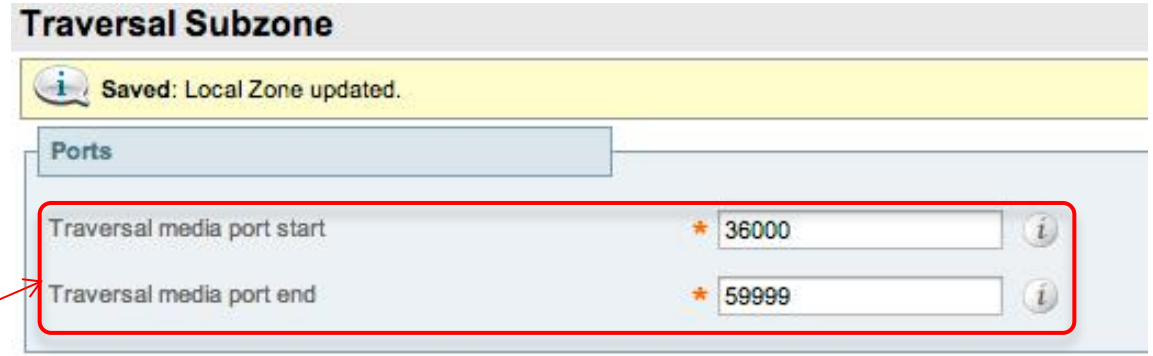
> Protocols > SIP



Firewall Configuration
Where to configure these ports?

- ExpressWay C > Configuration > Traversal Subzone

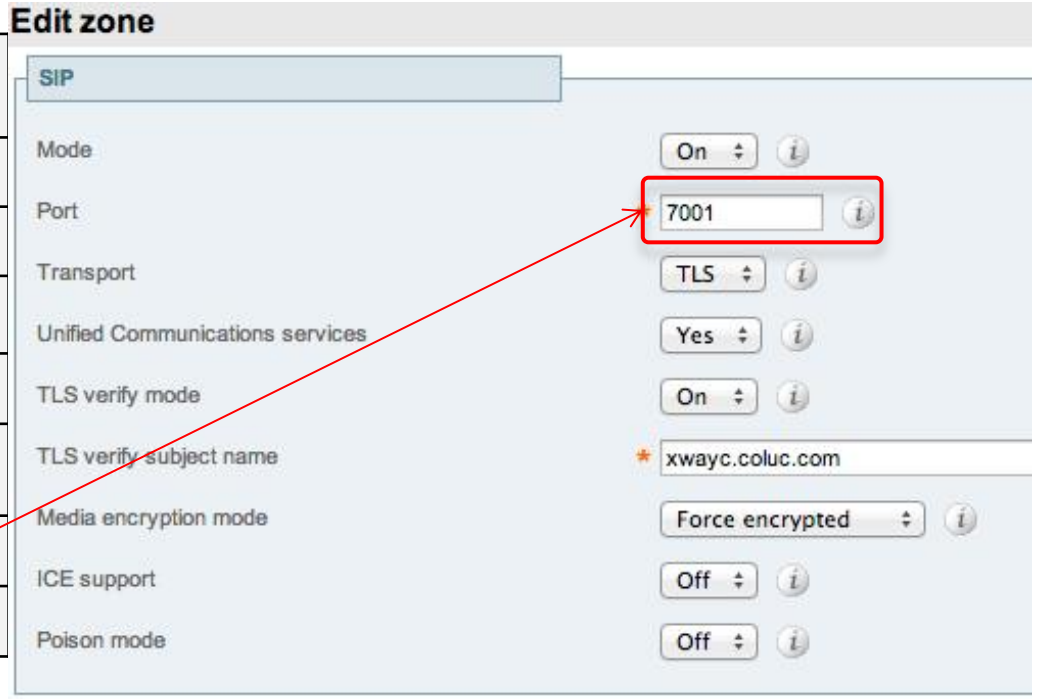
		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
	XMPP (IM and Presence)	TCP 7400	TCP **Ue** 30000 to 35999 *
	SSH (HTTP/S tunnels)	TCP **Ue** 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & **TLS_A** 25000 to 29999	TCP & **TLS_B** 7001
	SIP media	UDP **Y_C** 36000 to 59999 **	UDP **Y_E** 36000 to 59999 **



Firewall Configuration
Where to configure these ports?

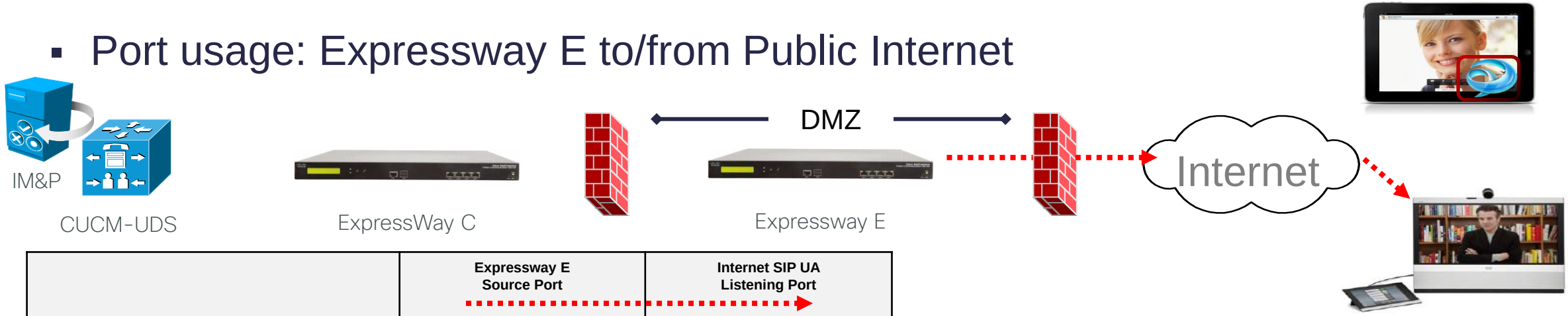
- ExpressWay E Zone > Configuration > Zone > Traversal

		ExpressWay C Source Port	ExpressWay E Listening Port
Management Control		Inbound and outbound calls	
Open Firewall		Private to DMZ	
IP Address		IP address of - ExpressWay C	IP address of - ExpressWay E
	XMPP (IM and Presence)	TCP 7400	TCP **Ue** 30000 to 35999 *
	SSH (HTTP/S tunnels)	TCP **Ue** 30000 to 35999 *	TCP 2222
	SIP signaling	TCP & **TLS_A** 25000 to 29999	TCP & **TLS_B** 7001
	SIP media	UDP **Y_C** 36000 to 59999 **	UDP **Y_E** 36000 to 59999 **



Firewall Configuration
To which ports does this translate?

- Port usage: Expressway E to/from Public Internet



		Expressway E Source Port	Internet SIP UA Listening Port
Management Control		Outbound to SIP UA in the Internet	
Open Firewall		DMZ to Internet	
IP Address		Public IP address of - ExpressWay E	IP address of - Any (or specific IP)
IP Ports	XMPP (IM and Presence)	N/A	N/A
	UDS (Provisioning and Phonebook)	N/A	N/A
	TURN Server Control	N/A	N/A
	SIP signaling	TLS 25000 to 29999	TLS **S** >= 1024
	Media	UDP Y_E 36000 to 59999 **	UDP **N** >= 1024

N = ExpressWay wait unit it receives media, then it sends its media to the IP port from which media was received (egress port of the media from the far end non SIP-aware firewall)

S = Source port, typically >=1024

Y_E = Configurable traversal media ports range (on Expressway/E)

** Default media ports range (X8.1) is 36000 – 59999 which configurable

Firewall Configuration
To which ports does this translate?

- Port usage: Expressway E to/from Public Internet

		Expressway C Listening Port	Internet SIP UA Source Port
Management Control		Inbound from SIP UA in the Internet	
Open Firewall		Internet to DMZ	
IP Address		IP address of - VCS Expressway	IP address of - Any (or specific IP)
IP Ports	XMPP (IM and Presence)	TCP 5222	TCP **S** >= 1024
	UDS (Provisioning)	TCP 8443	TCP **S** >= 1024
	TURN Server Control	UDP 3478	UDP **S** >= 1024
	SIP signaling	TLS 5061	TLS **S** >= 1024
	Media	UDP Y_E 36000 to 59999 **	UDP **N** >= 1024

N = ExpressWay wait unit it receives media, then it sends its media to the IP port from which media was received (egress port of the media from the far end non SIP-aware firewall)

S = Source port, typically >=1024

Y_E = Configurable traversal media ports range (on Expressway/E)

** Default media ports range (X8.1) is 36000 – 59999 which configurable

Firewall Configuration
To which ports does this translate?

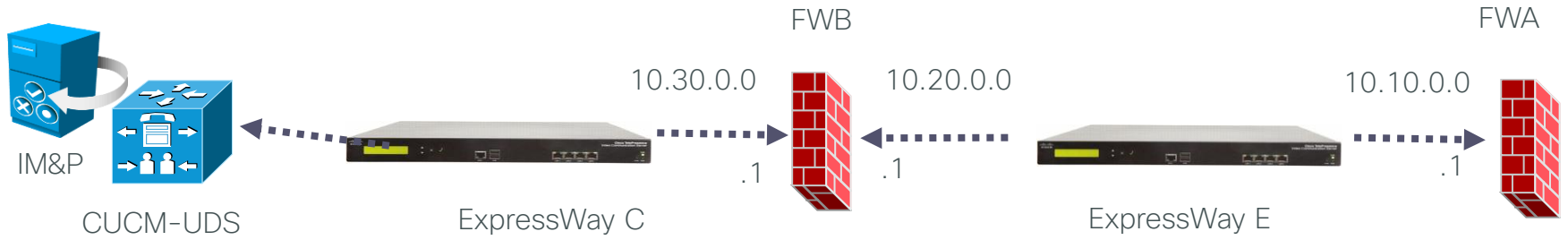
- Port usage: ExpressWay C to Unified CM and IM&P

		CUCM&CUP System Listening Port	ExpressWay C Source Port
Management Control		Private Network	
Open Firewall		N/A	
IP Address		IP address of - Unified CM - IM & Presence Server	IP address of - ExpressWay C
IP Ports	XMPP (IM and Presence)	TCP 7400 (IM&P Server)	TCP **Ue** 30000 to 35999 *
	UDS (Provisioning and Phonebook)	TCP 8443 (CUCM Server)	TCP **Ue** 30000 to 35999 *
	TFTP	TCP 6970 (TFTP Server)	TCP **Ue** 30000 to 35999 *
	CUC (Voicemail)	TCP 443 (CUC server)	TCP **Ue** 30000 to 35999 *

Ue = Configurable TCP ephemeral port range

***** Default ephemeral ports range (X8.1) for is 30000 – 35999 which configurable

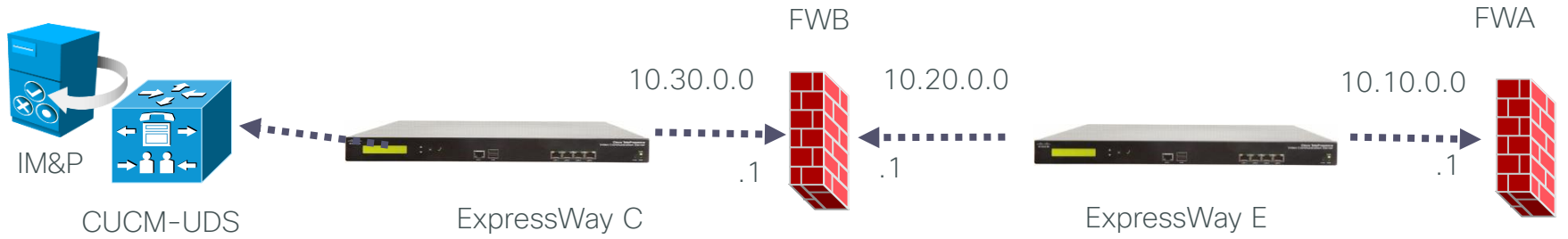
Firewall Setup
Dual NIC consideration



- ExpressWay-E has default GTW 10.10.0.1
- When FWB does NAT for 10.30.0.0 there is no problem
- When FWB does no NAT for 10.30.0.0 a static route needs to be added

  xCommand RouteAdd Address: 10.30.0.0 PrefixLength: 24 Gateway: 10.20.0.1 Interface: LAN1

Firewall Setup
Dual NIC consideration with static NAT & NAT Reflection



- ExpressWay-C traversal client points to public IP on ExpressWay-E
- FWA must support NAT Reflection

Firewall Setup
Port Status and Configuration

- Maintenance > Tools > Port Usage

Local inbound ports

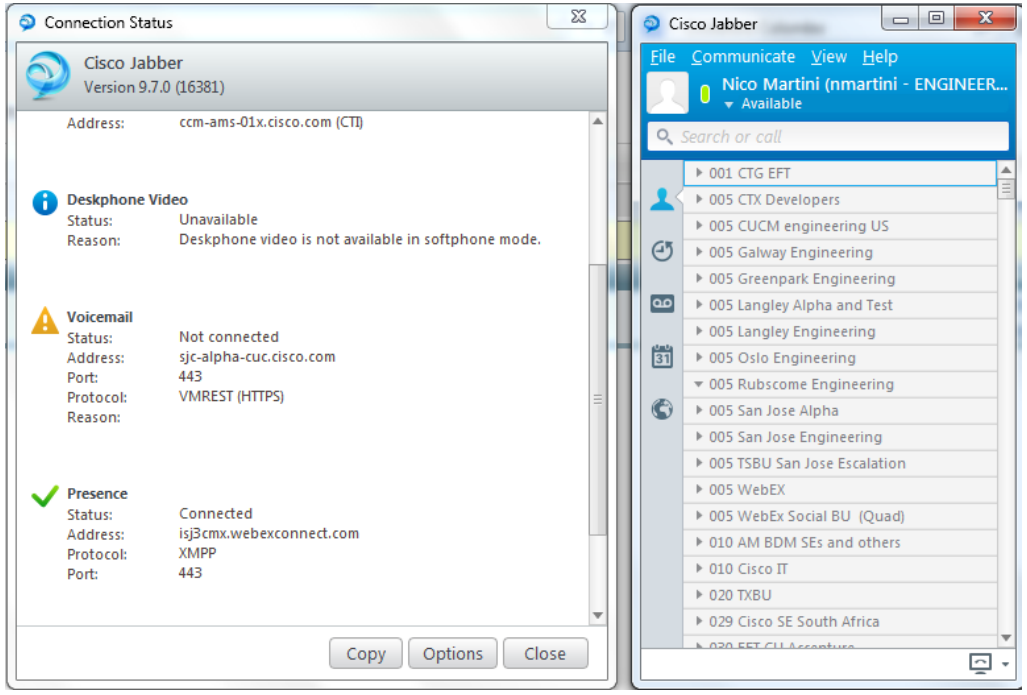
You are here: Maintenance ▸ Tools ▸ Port usage ▸ Local inbound ports

Type	Description	Protocol	IP address	IP port	Transport	Actions
Administration	SSH port		10.48.55.99	22	TCP	Not configurable
Administration	HTTP port		10.48.55.99	80	TCP	Not configurable
Administration	HTTPS port		10.48.55.99	443	TCP	Not configurable
Administration	SNMP port		10.48.55.99	161	UDP	Not configurable
H.323	Multicast gatekeeper discovery port	H.323	10.48.55.99	1718	UDP	Not configurable
H.323	Call signaling TCP port	H.323	10.48.55.99	1720	TCP	View/Edit
H.323	Call signaling port range	H.323	10.48.55.99	15000-19999	TCP	View/Edit
H.323	Registration UDP port	H.323	10.48.55.99	1719	UDP	View/Edit
SIP	TCP port	SIP	10.48.55.99	5060	TCP	View/Edit
SIP	TLS port	SIP	10.48.55.99	5061	TCP	View/Edit
Media	Media port range	RTP,RTCP	10.48.55.99	50000-54999	UDP	View/Edit
Expressway	H.323 Assent call signaling port	H.323	10.48.55.99	2776	TCP	View/Edit
Expressway	H.323 H.460.18 call signaling port	H.323	10.48.55.99	2777	TCP	View/Edit
Traversal server zone	TraversalZone	SIP	10.48.55.99	7001	TCP	View/Edit
Unified Communications	SSH tunnels	SSH	10.48.55.99	2222	TCP	Not configurable
Unified Communications	HTTP proxy	HTTP	10.48.55.99	8443	TCP	Not configurable
Unified Communications	XMPP proxy client port	XMPP	10.48.55.99	5222	TCP	Not configurable
Unified Communications	XMPP proxy router port	XMPP	10.48.55.99	7400	TCP	Not configurable

Export to CSV

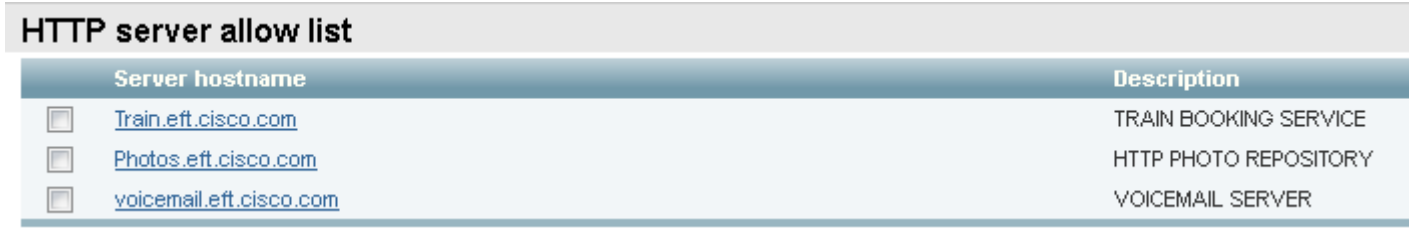
HTTP Server Allow list ExpressWay C

- Some services are relying on HTTP Reverse Proxy functionality in Expressways Example :
  - “Unity Connection Voicemail Player”
  - “Customized Jabber HTTP Contact Photos”
  - “Customizes Jabber plugins”



HTTP Server Allow list
ExpressWay C

- > Configuration > Unified Communications > Configuration



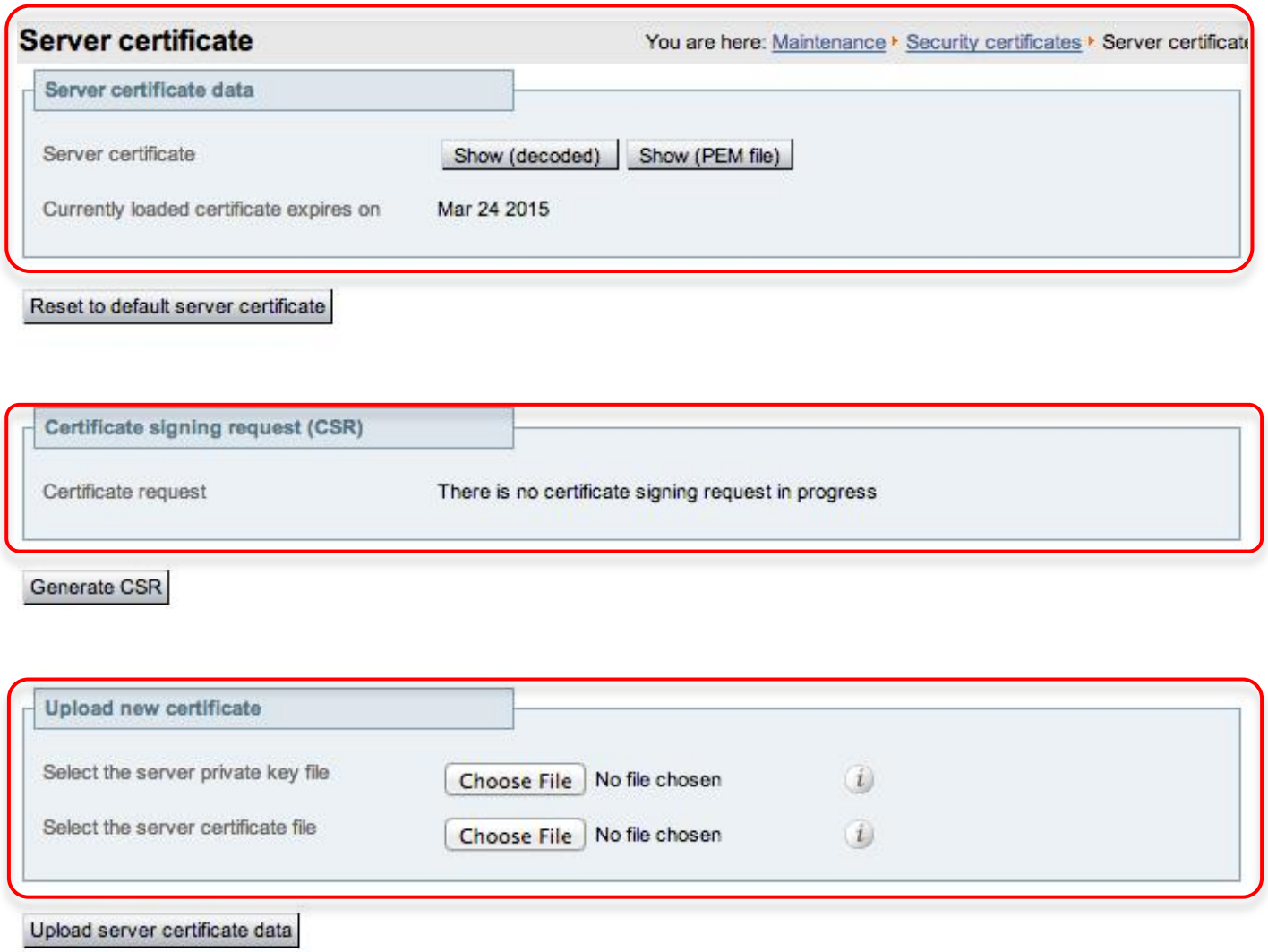
- The hostname or IP address of an HTTP server that a Jabber client located outside of the enterprise is allowed to access.

  Access is granted if the server portion of the client-supplied URI matches the name entered here, or if it resolves via DNS lookup to an IP address specified here.

Certificates

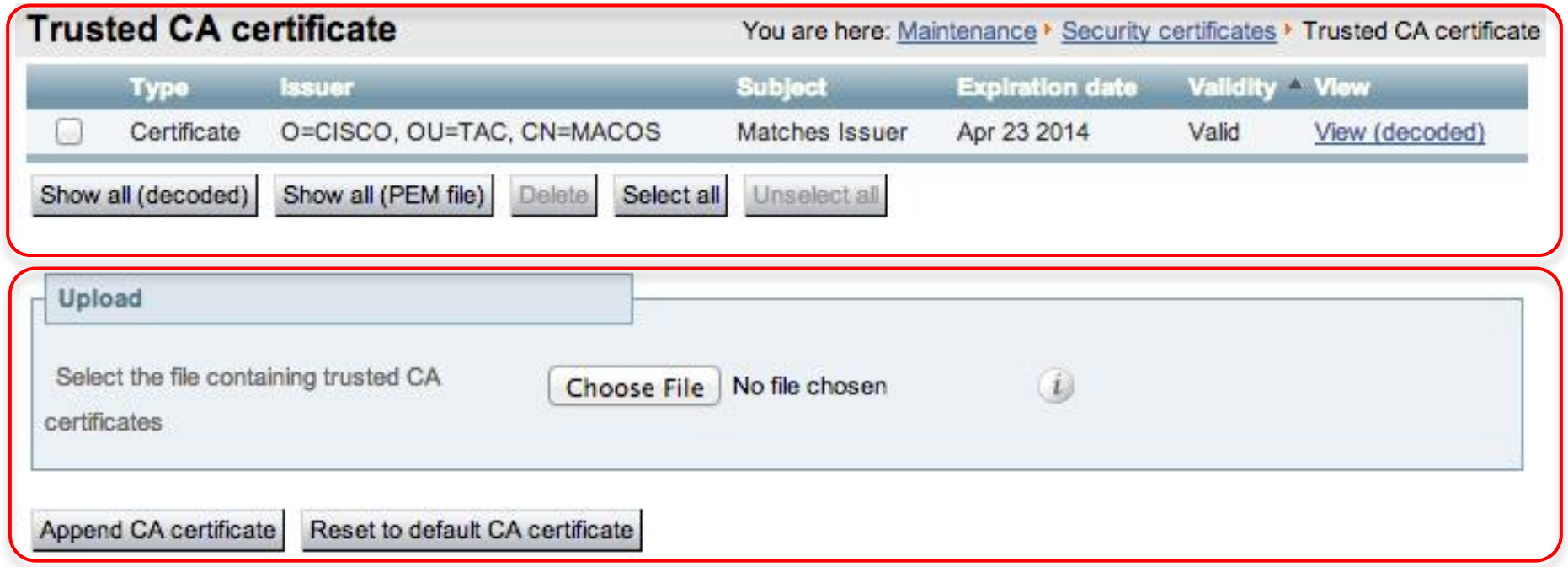
Certificates

- Maintenance > Security Certificate > Server Certificate



Certificates

- Maintenance > Security Certificate > Trusted CA Certificate



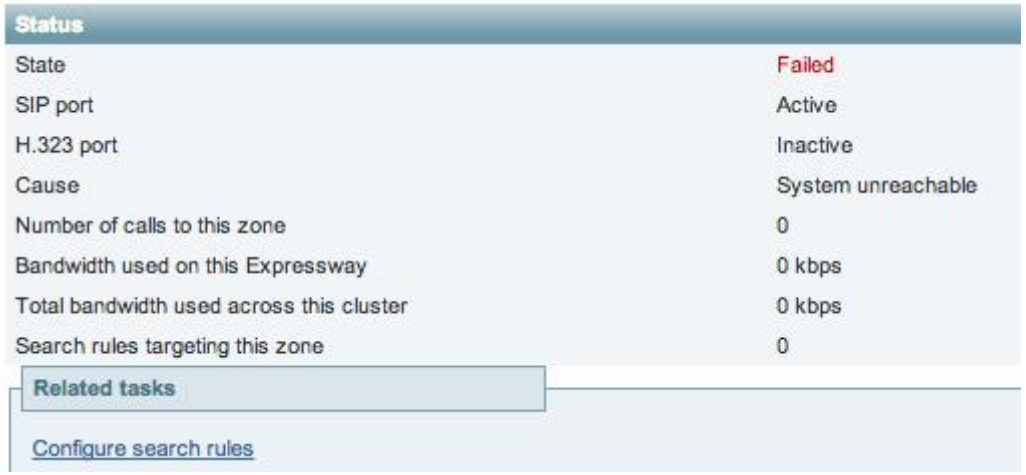
ExpressWay C – Certificate Requirements

- CA Signed

  - Must be CA signed
  - Used with ExpressWay E for traversal zone connection
  - Used with CUCM when endpoint security mode is Authenticated or Encrypted (TLS transport used)
  - CA Root must be appended to “Trusted CA certificate” on both ExpressWay’s
  - CA Root must be uploaded to Callmanager-trust store on every node in the cluster

ExpressWay C – Certificate Requirements
CA Root not uploaded on ExpressWay E

- Traversal Zone State Failed



Status	
State	Failed
SIP port	Active
H.323 port	Inactive
Cause	System unreachable
Number of calls to this zone	0
Bandwidth used on this Expressway	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

Related tasks

Configure search rules

- Expressway-C Diagnostics logs (traversal client)

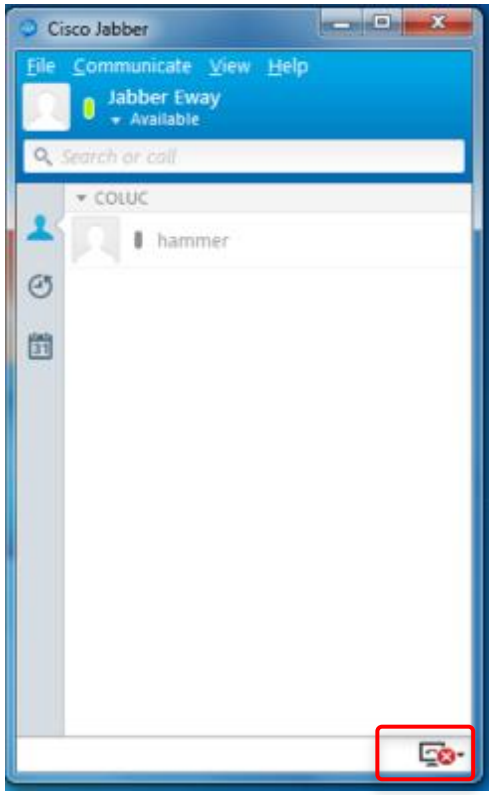
  xwayc tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25016" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="xwaye.coluc.com" Level="1" UTCTime="2014-03-24 17:33:30,872”

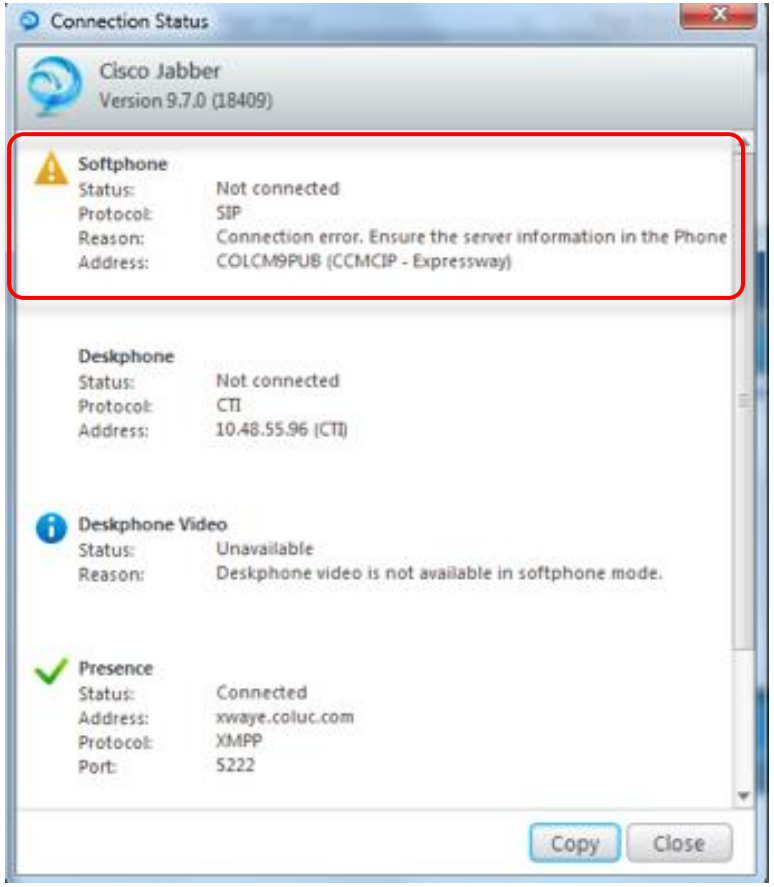
- Expressway Event logs

Results	
2014-03-24T17:36:30+00:00	tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25025" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca " Protocol="TLS" Common-name="xwaye.coluc.com" Level="1" UTCTime="2014-03-24 17:36:30,872"

ExpressWay C – Certificate Requirements
CA Root not uploaded on CUCM

- Softphone Registration fails (other will work) when endpoint security settings are authenticated or encrypted





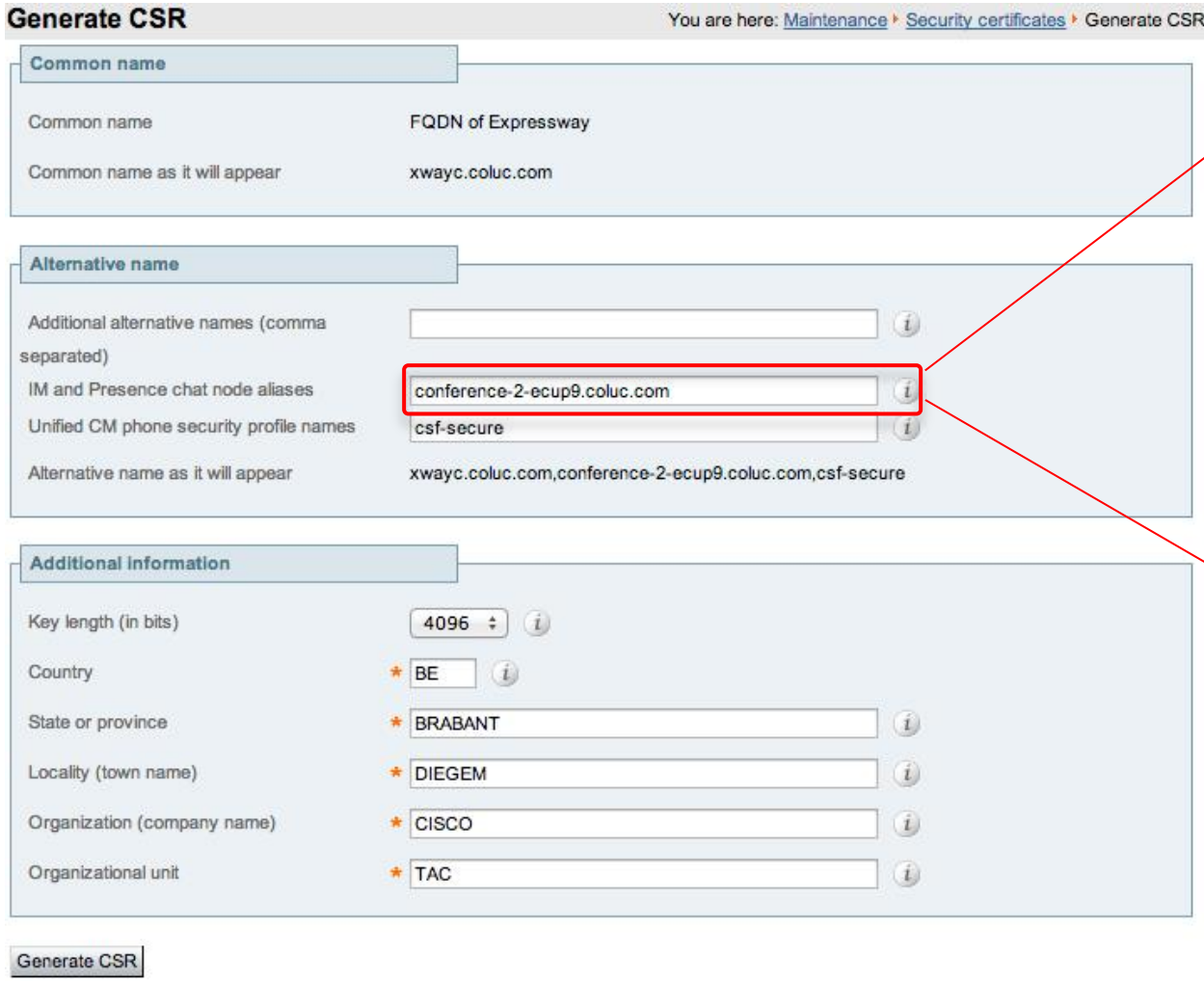
ExpressWay C – Certificate Requirements

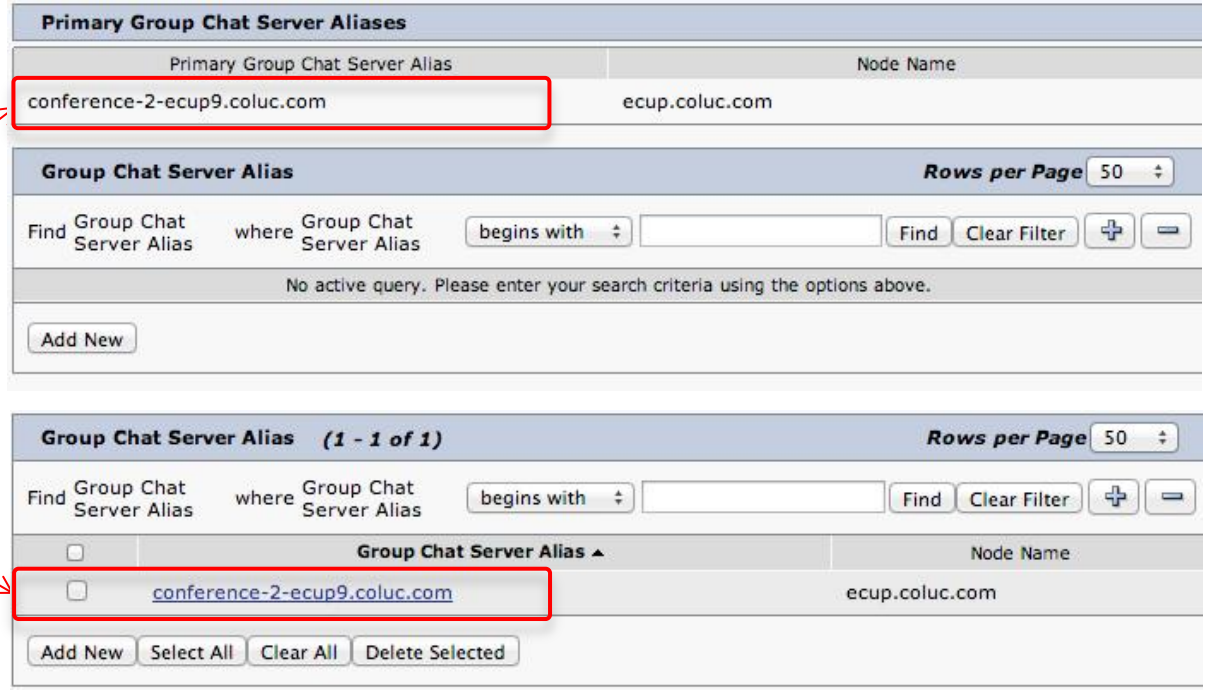
- SAN must include ‘Chat node alias’ from IM&P server (CUP)

  - Required for XMPP federation
  - Get auto-added in CSR after IM&P discovery
  - For manual configuration go to CUPADMIN > Messaging > Group Chat Server Alias Mapping, click find.

ExpressWay C – Certificate Requirements

CUPADMIN > Messaging > Group Chat Server Alias Mapping



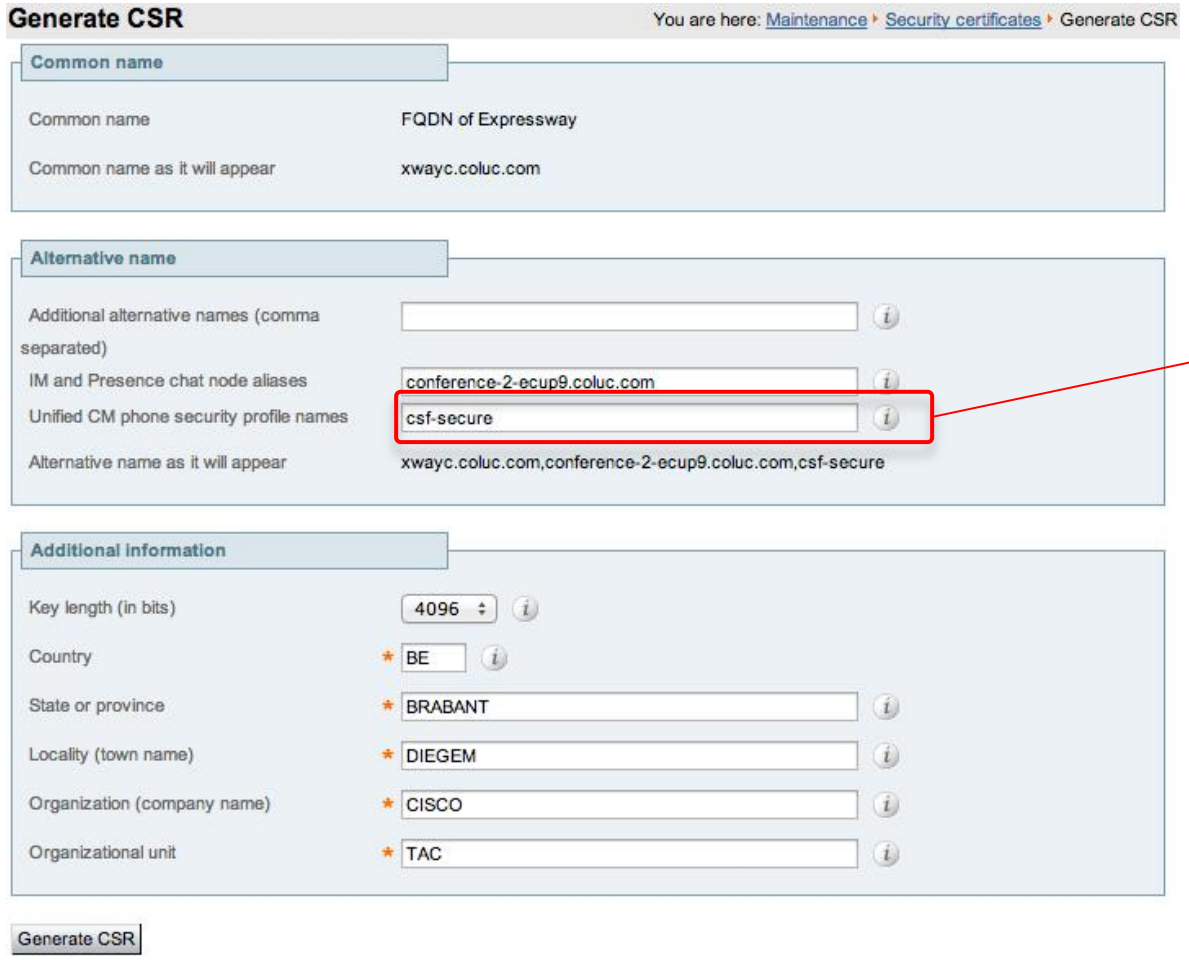


ExpressWay C – Certificate Requirements

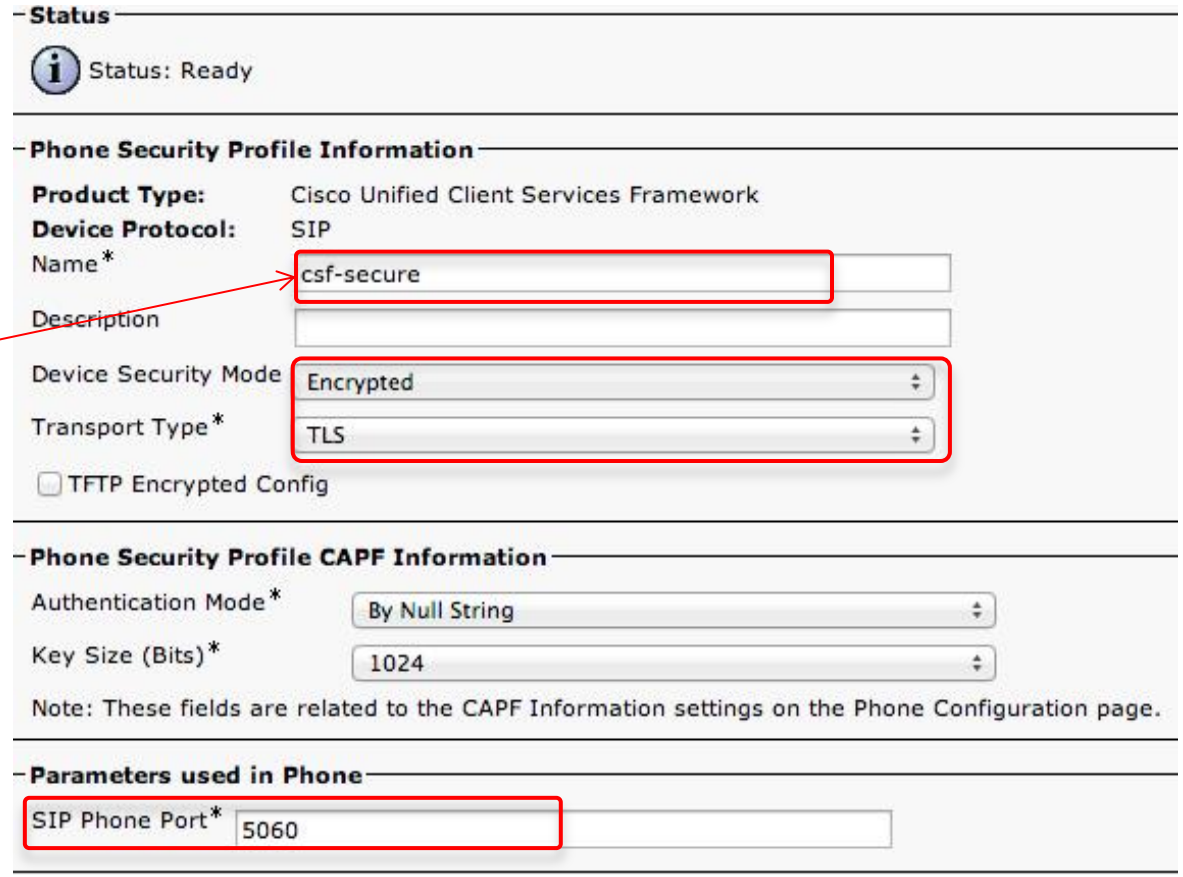
- SAN must include ‘Device Security Profile Name’

  - Required for CUCM to accept the TLS Connection
  - X509 from certificate presented is that one of ExpressWay C
  - CUCM needs to validate using SAN matching the security profile name
  - Some (public) CA’s do not allow hostname in SAN
  If so, the profile name must have FQDN format

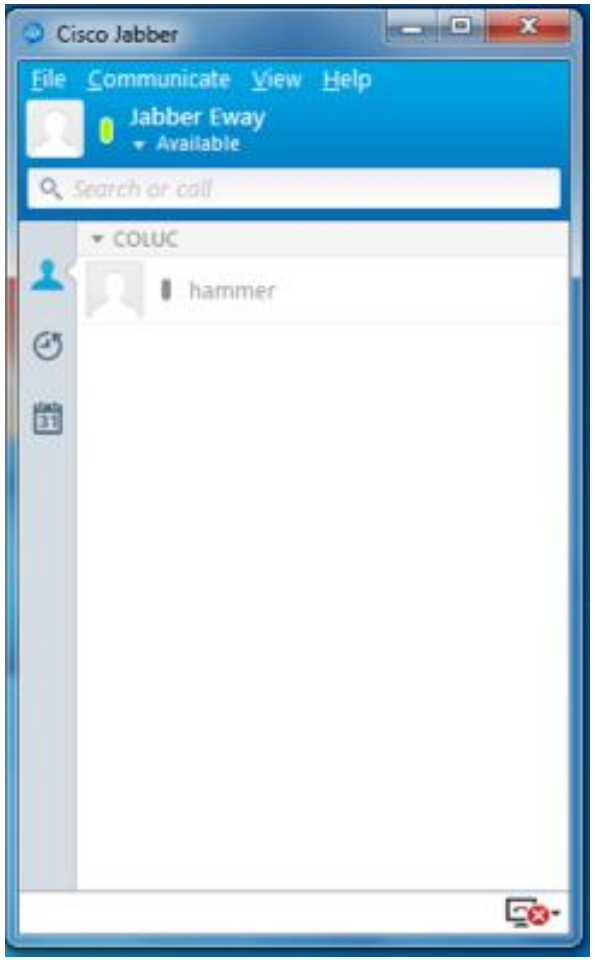
ExpressWay C – Certificate Requirements

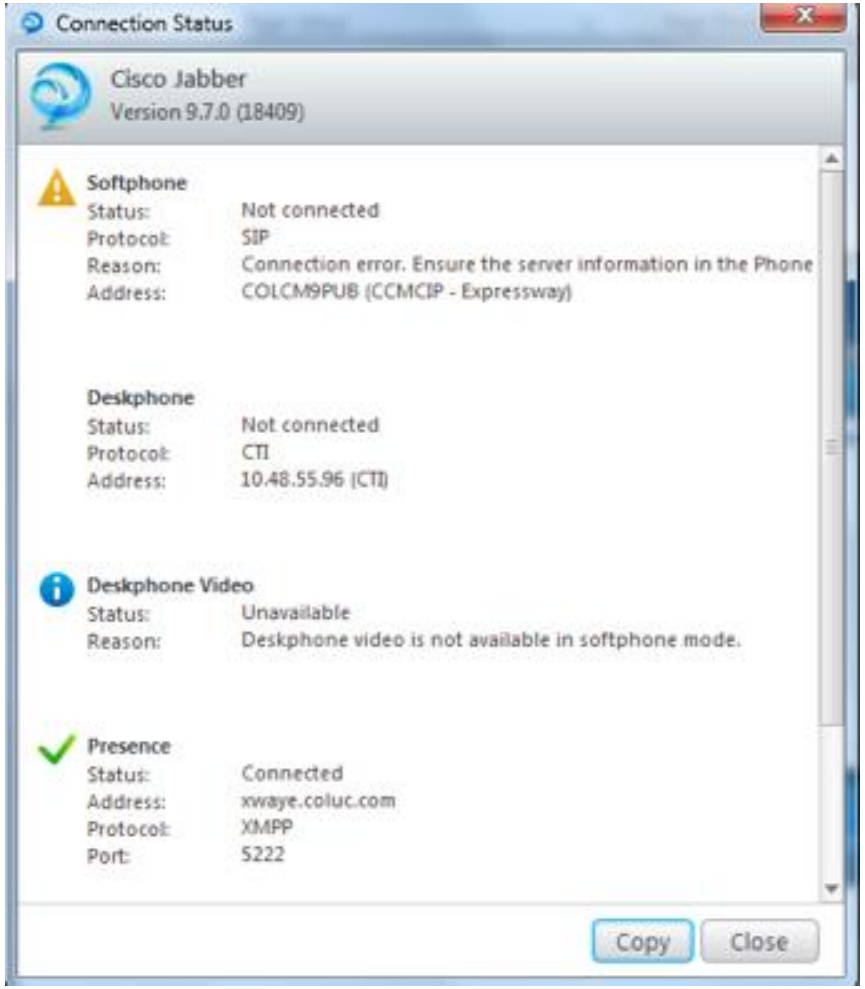


System > Security > Phone Security Profile



ExpressWay C – Certificate Requirements
Security Profile not added as SAN





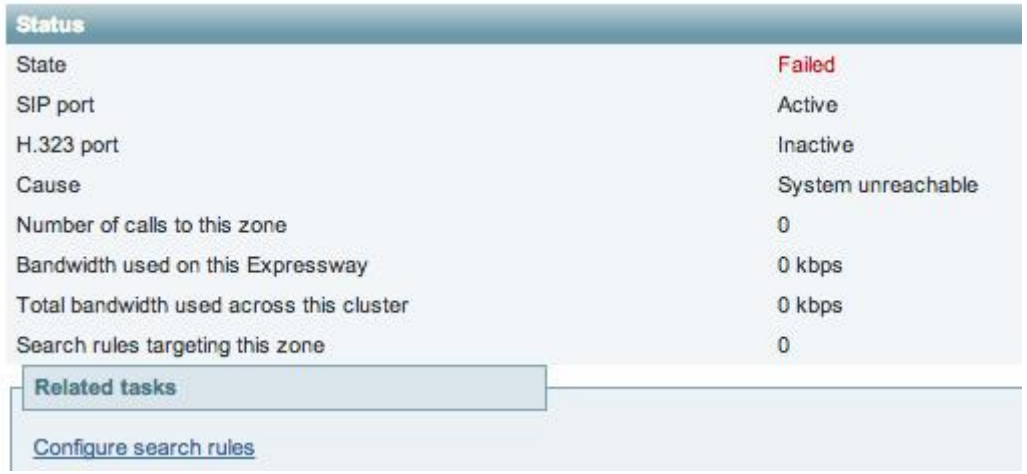
ExpressWay E – Certificate Requirements

- CA Signed

  - Must be CA signed
  - Used with ExpressWay C for traversal zone connection
  - CA Root must be appended to “Trusted CA certificate” on both ExpressWay’s

ExpressWay E – Certificate Requirements
CA root not uploaded to ExpressWay C

- Traversal Zone State



- ExpressWay E diagnostic logs
  xwaye tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25006" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Level="1" UTCTime="2014-03-25 09:52:36,680”

- ExpressWay E event logs

Common

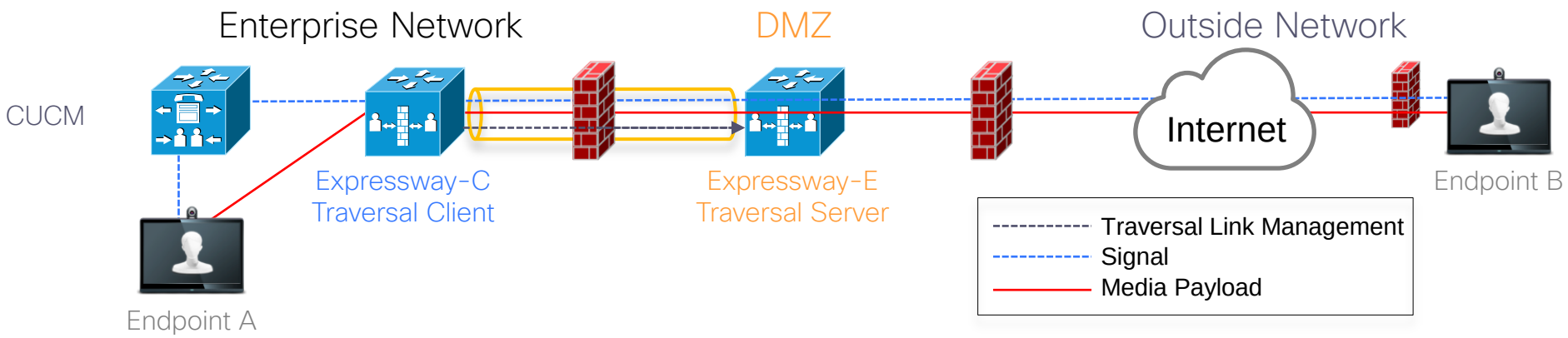
- If Expressway does not have a valid signed certificate that contains either the FQDN or domain of Expressway, then this fails and the Jabber client fails to log in.
- If this issue occurs, the customer should use the Certificate Signing Request (CSR) tool on Expressway, which automatically includes the FQDN of Expressway as a Subject Alternative Name (SAN).
- *Expressway-C Server Certificate Requirements:*
- The **Chat Node Aliases** configured on the IM&P servers. This is required if you perform Extensible Messaging and Presence Protocol (XMPP) federation. Expressway-C should automatically include these in the CSR provided that an IM&P server has already been discovered on Expressway-C.
- The names in FQDN format of all **Phone Security Profiles** in CUCM configured for TLS and used on devices configured for MRA. This allows for secure communication between the CUCM and Expressway-C for the devices that use those Phone Security Profiles.

- *Expressway-E Server Certificate Requirements:*
- All domains configured for Unified Communications. This includes the domain of Expressway-E and C, email address domain configured for Jabber, and any Presence domains.
- The **Chat Node Aliases** configured on the IM&P servers. This is required if you perform XMPP federation.

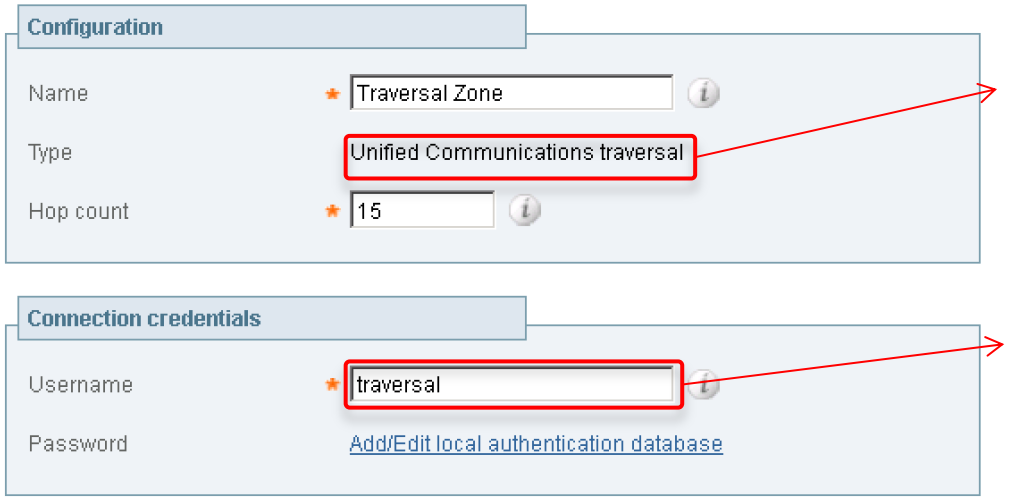
Traversal Zone Setup

Traversal Zone Setup
Firewall Traversal

- Expressway-E is traversal server in DMZ
- Expressway-C is traversal client inside the network
- Establish traversal link between both using traversal zone configuration



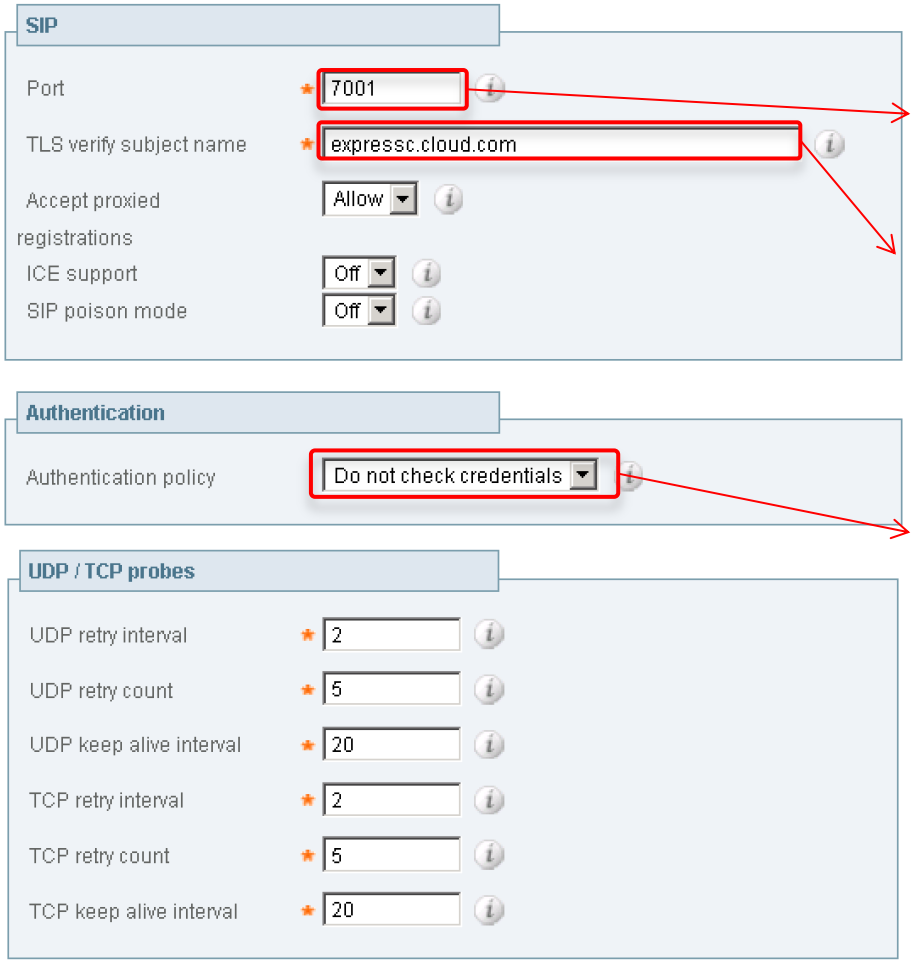
Traversal Zone Setup
ExpressWay E – Traversal Server



Select Type : Unified Communications traversal

Configure username to be used by Traversal Client to authenticate with server

Traversal Zone Setup
ExpressWay E – Traversal Server

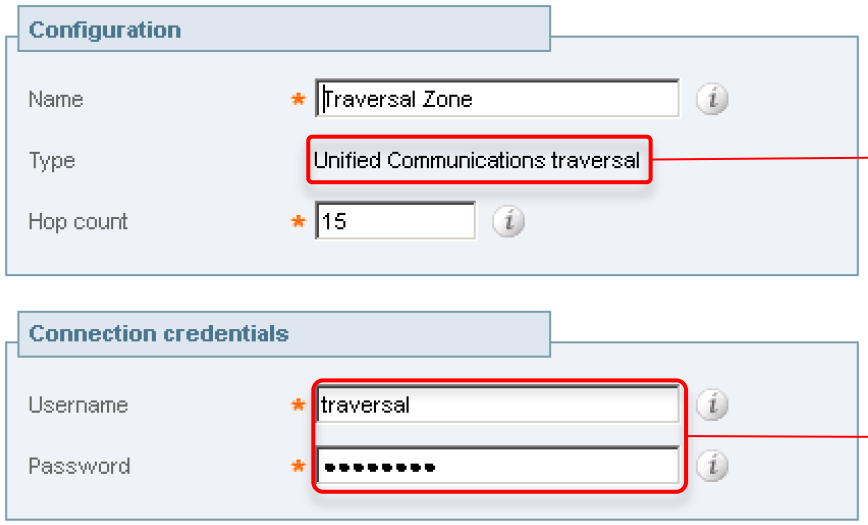


Port is default 7001, listening port for traversal client connection

Must match CN from Certificate presented by Traversal Client (ExpressWay C)

Must be set to ‘Do not check ..’
(expressway does not register any endpoint)

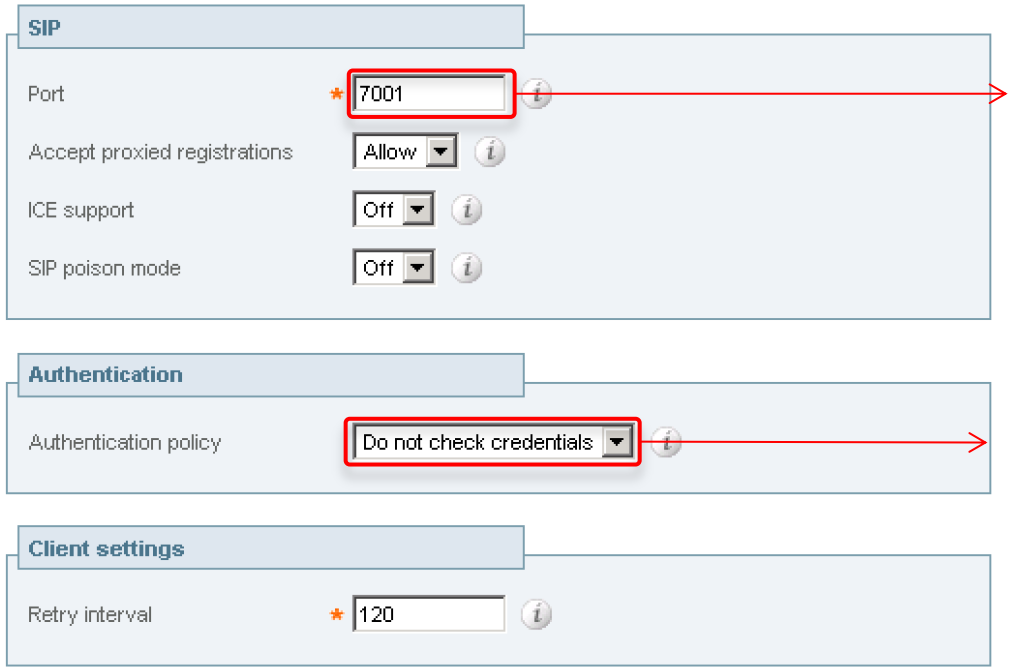
Traversal Zone Setup
ExpressWay C – Traversal Client



Type: Unified Communication traversal

Configure same username and password as added on the Traversal Server (Expressway E)

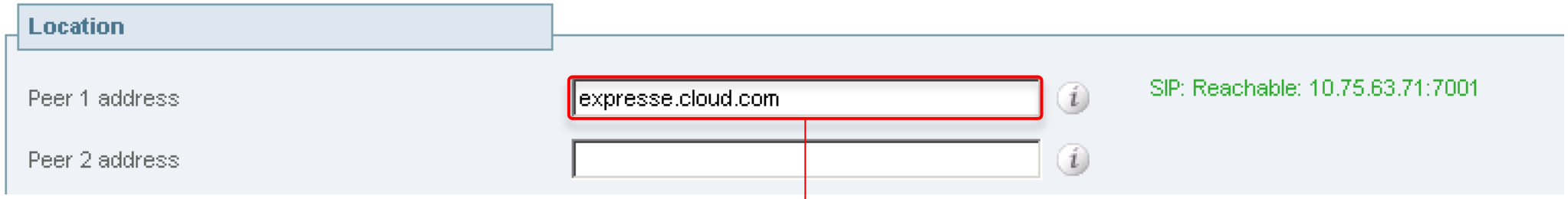
Traversal Zone Setup
ExpressWay C – Traversal Client



Destination port Traversal Server is listening on

Must be set to ‘Do not check ..’ (expressway does not register any endpoint)

Traversal Zone Setup
ExpressWay C – Traversal Client



- Must be FQDN
- Must be DNS resolvable

Traversal Zone Setup
Peer Address not matching CN

- Peer Address configured as IP address

- ExpressWay diagnostic logs

  2014-03-25T14:08:16+00:00 xwayc tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25697" Dst-ip="10.48.55.99" Dst-port="7001" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.55.99" Level="1" UTCTime="2014-03-25 14:08:16,699”

- ExpressWay Event logs

Traversal Zone Setup
Peer Address not matching CN

- Peer Address/FQDN not matching CN

- ExpressWay diagnostic logs

  2014-03-25T14:16:36+00:00 xwayc tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25714" Dst-ip="10.48.55.99" Dst-port="7001" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="xwy.coluc.com" Level="1" UTCTime="2014-03-25 14:16:36,699"

- ExpressWay Event logs

Traversal Zone Setup
Password incorrect

- Traversal Client will show for this zone

- ExpressWay C diagnostic logs

Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="xwaye.coluc.com" Type="A and AAAA”
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4"TCP"10.48.55.99'] (A/AAAA) Number of relevant records retrieved: 1”
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99" Dst-port="7001" Detail="TCP Connecting”
Module="network.tcp" Level="DEBUG": Src-ip="10.48.55.98" Src-port="25723" Dst-ip="10.48.55.99" Dst-port="7001" Detail="TCP Connection Established"
….

Password incorrect

- ExpressWay C event log

Results	
2014-03-25T14:19:56+00:00	tvcs: Event="External Server Communications Failure" Reason="gatekeeper timed out" Service="NeighbourGatekeeper" Dst-ip="10.48.55.99" Dst-port="7001" Detail="name:xwaye.coluc.com" Protocol="TCP" Level="1" UTCTime="2014-03-25 14:19:56,705"

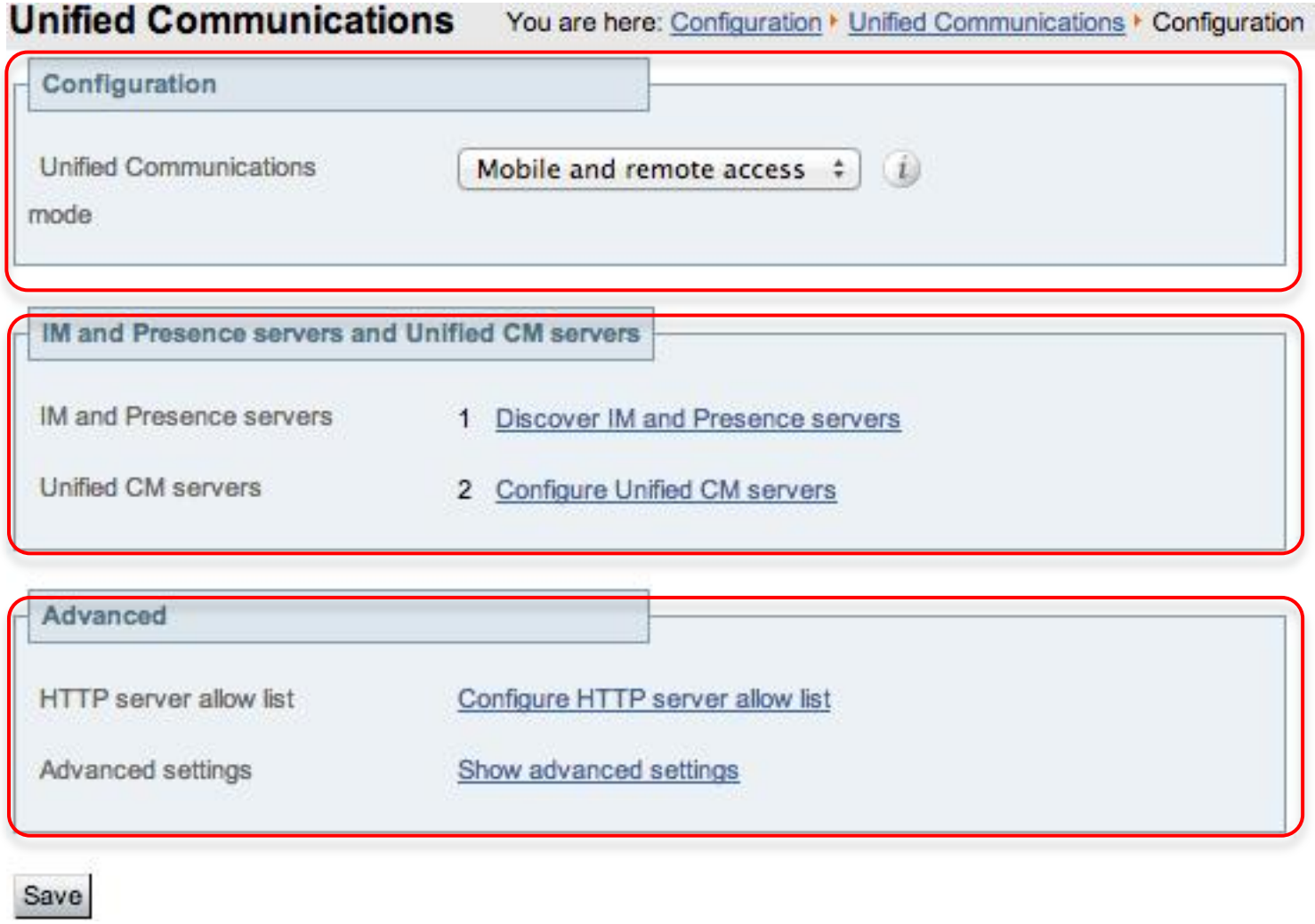
- ExpressWay E event log

Results	
2014-03-25T14:36:56+00:00	tvcs: Event="Authentication Failed" Service="SIP" Src-ip="10.48.55.98" Src-port="25723" Detail="Incorrect authentication credential for user" Protocol="TLS" Method="OPTIONS" Level="1" UTCTime="2014-03-25 14:36:56,694"

UC Server Discovery

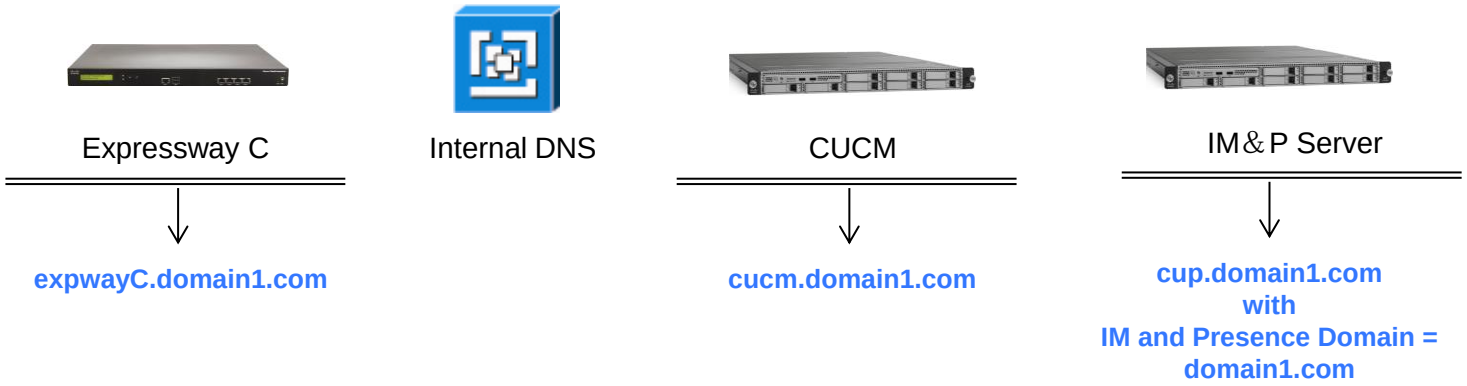
UC Server Discovery

Configuration > Unified Communications

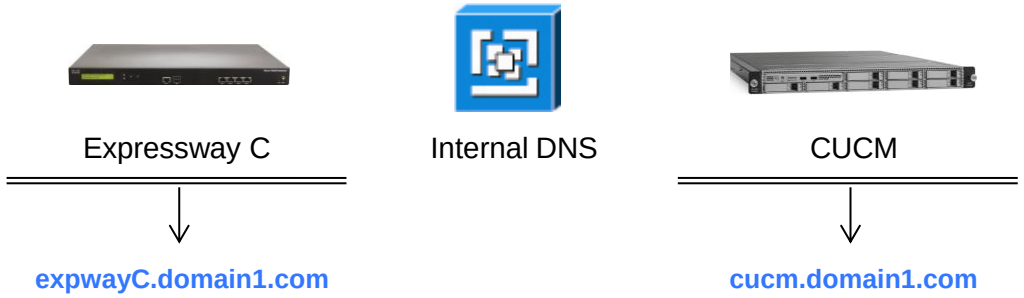


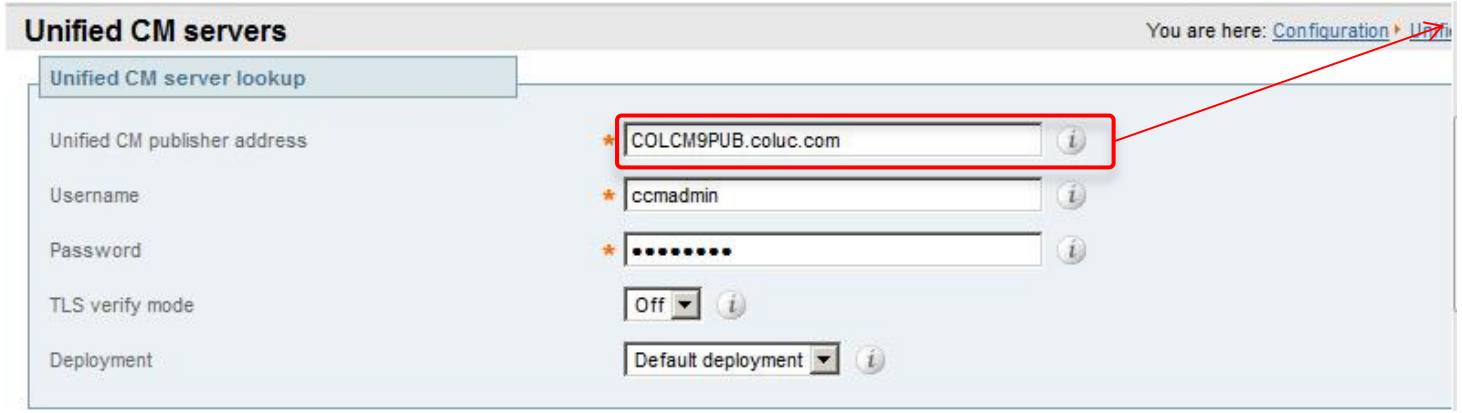
ExpressWay – Mobile and Remote Access
UC Server discovery

- Scenario 1
  - CUCM set to none-secure



ExpressWay Mobile and Remote Access – Scenario 1 CUCM Server Discovery

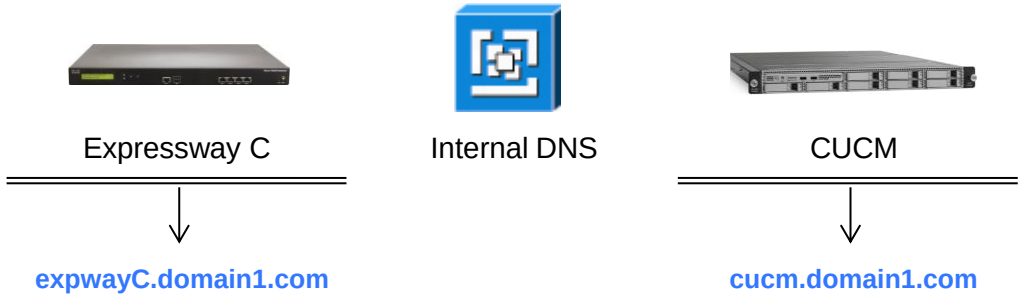


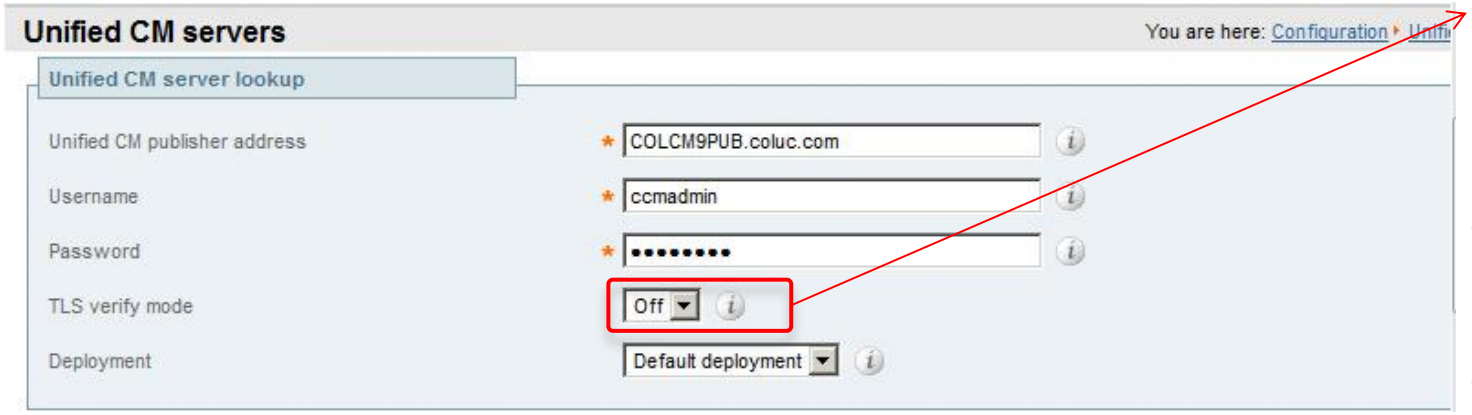


What do I enter here?

- When TLS verify mode is On > Must match CN from Tomcat Certificate
- When TLS verify mode Off > IP Address Publisher or Hostname Publisher or FQDN Publisher

ExpressWay Mobile and Remote Access – Scenario 1 CUCM Server Discovery

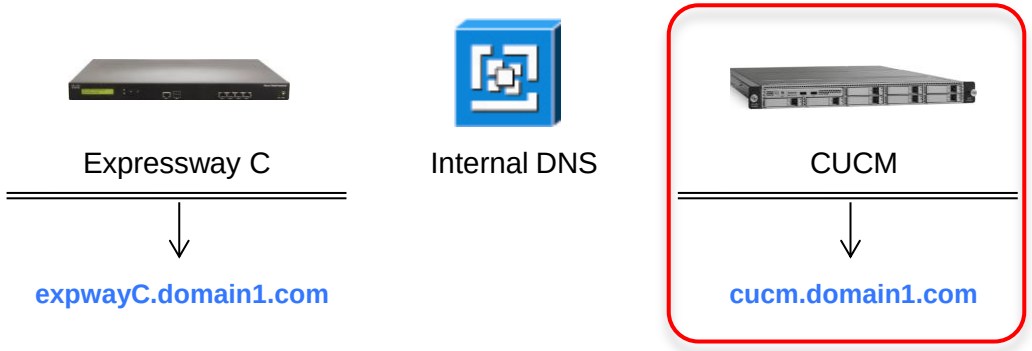




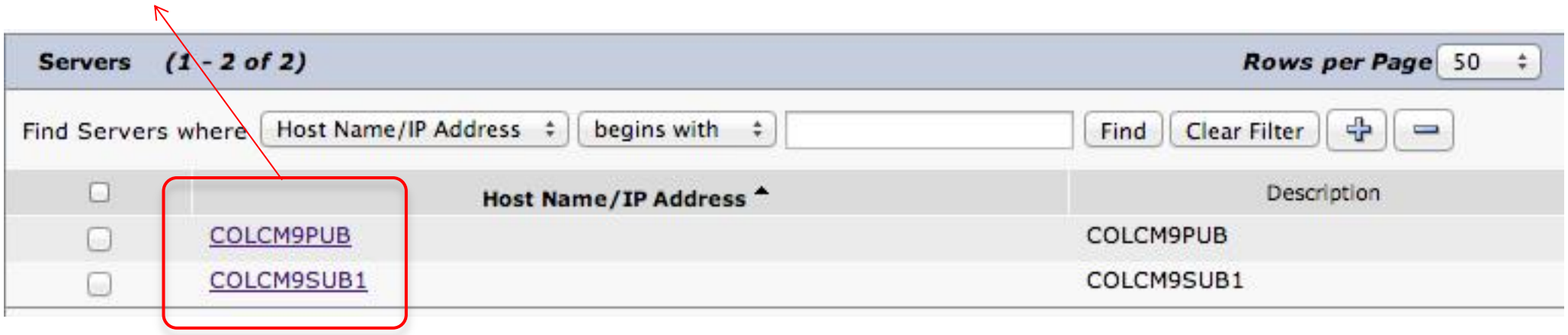
Set to off for non-secure
When set to 'On'
what other configuration is required?

- Self Signed Tomcat Certificate must be appended to "Trusted CA Cert"
Or
- CA certificate must be appended
(And address must match CN from Tomcat certificate)

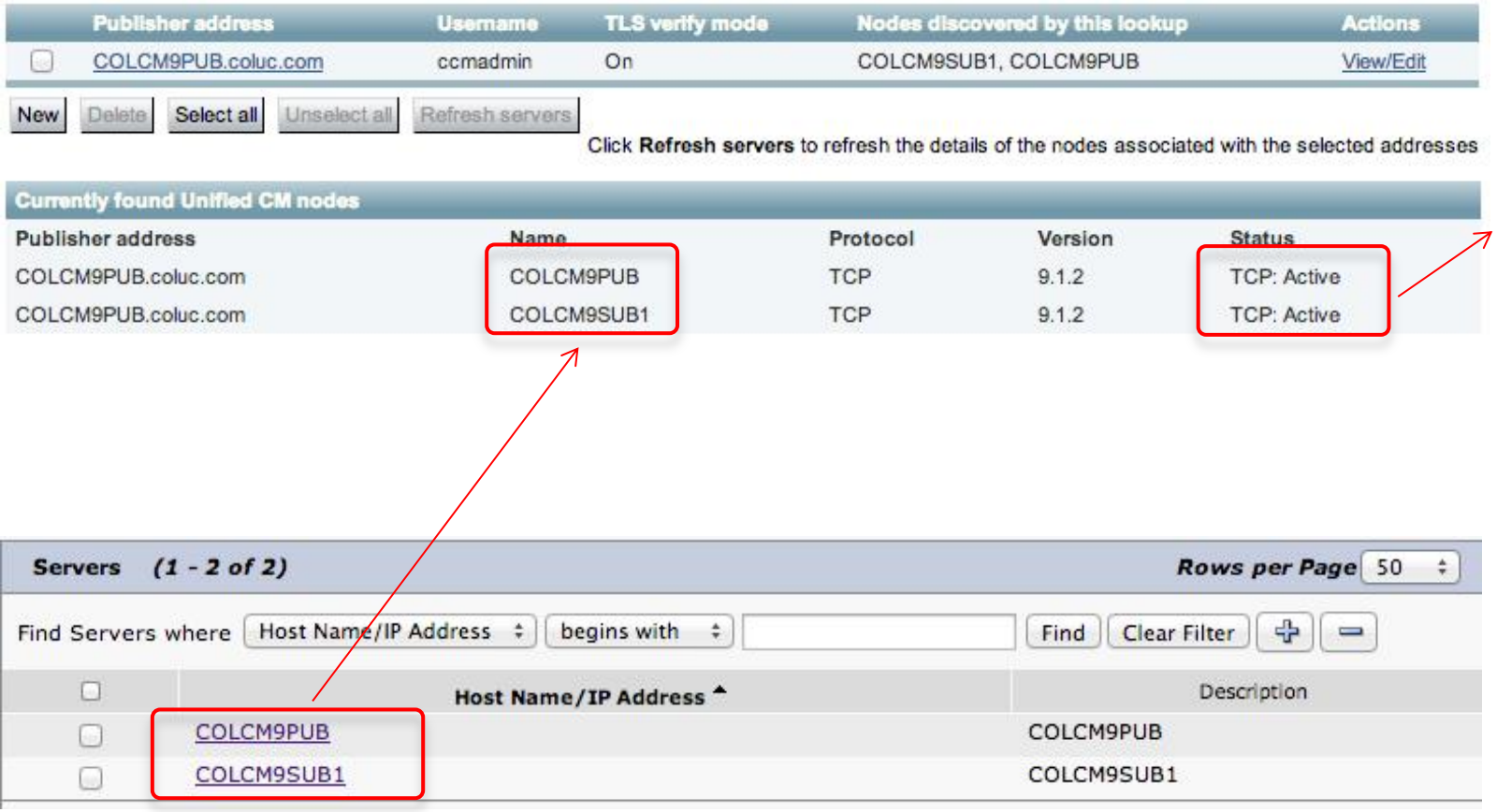
ExpressWay Mobile and Remote Access – Scenario 1 CUCM Server Discovery



How does Server configuration on CUCM impact the discovery?



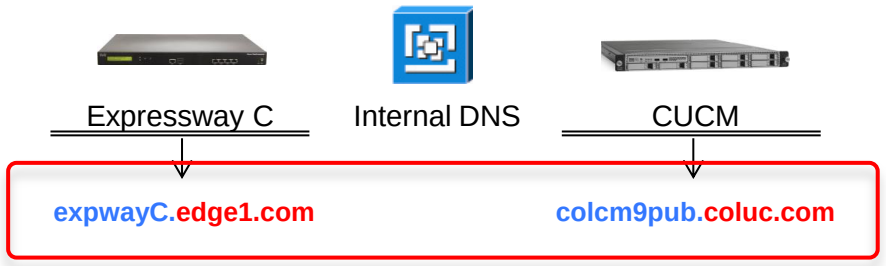
ExpressWay Mobile and Remote Access – Scenario 1
CUCM Server Discovery

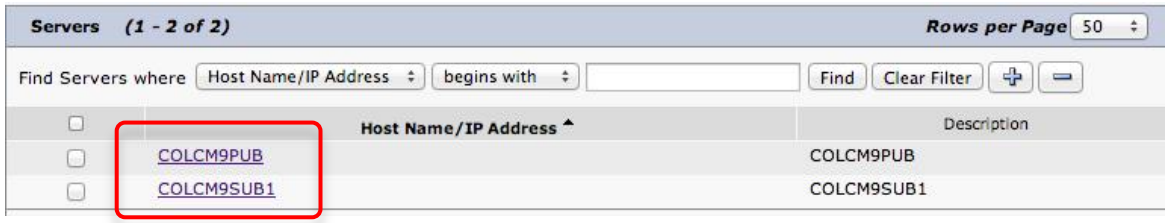


- When hostname is returned shows Active when xway can DNS resolve <hostname>@<domain Xway>
  or
  <hostname>
  where <hostname> is
  what is configured in CCMADMIN

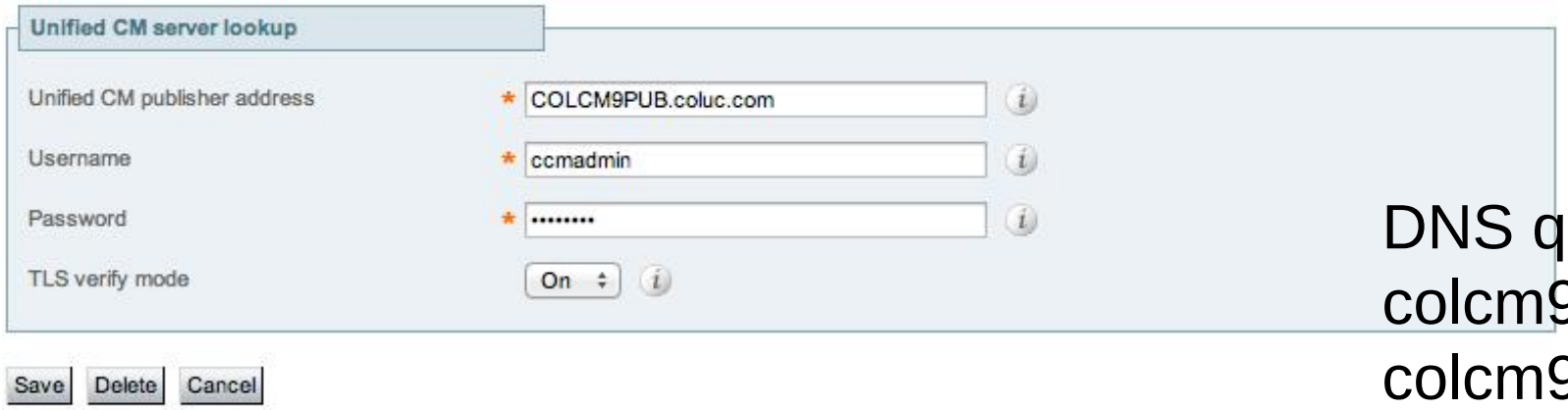
- This creates a problem when Expressway/VCS and CUCM servers are in different domains

ExpressWay Mobile and Remote Access – Scenario 1
CUCM Server Discovery – Different Server Domain

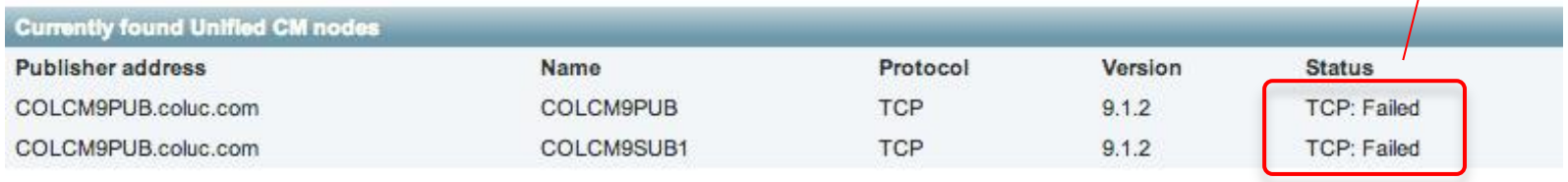




=



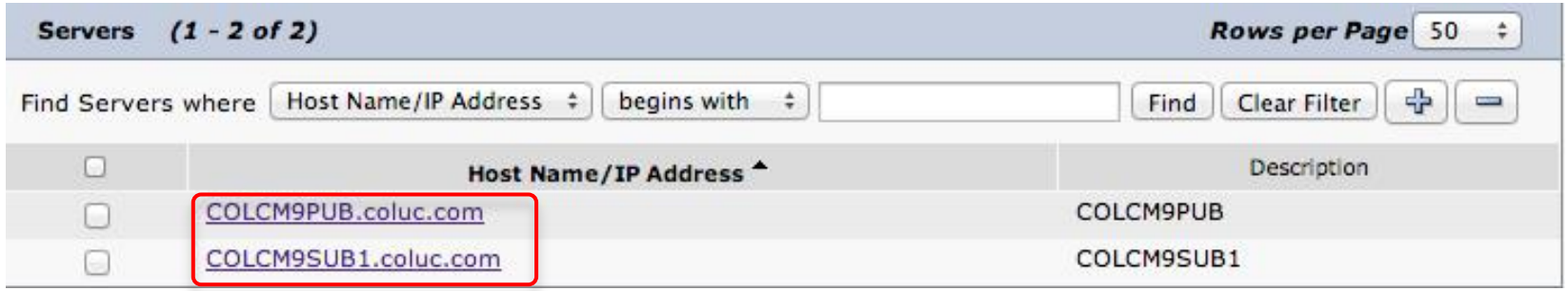
DNS query fails for
colcm9pub.edge.com
colcm9pub



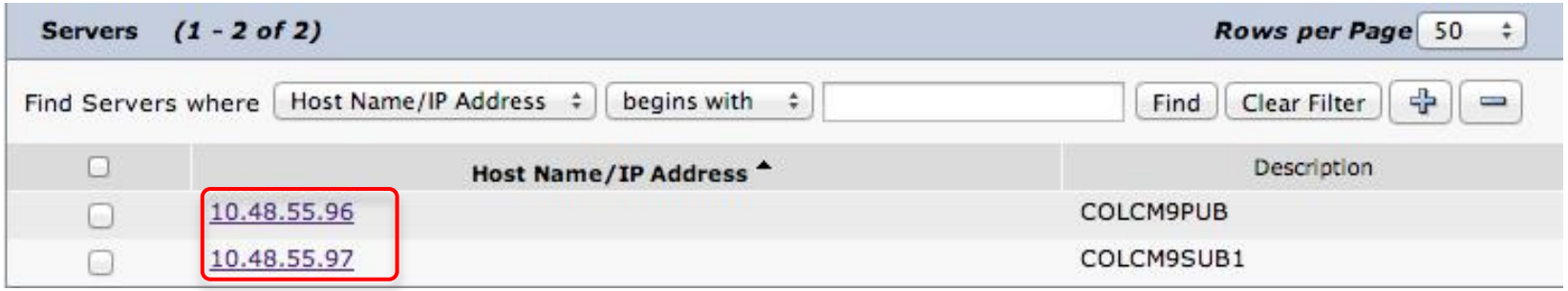
ExpressWay Mobile and Remote Access – Scenario 1 CUCM Server Discovery

- How to solve?

  1) Use FQDN for server configuration on CCMADMIN



  2) Use IP address for server configuration on CCMADMIN



ExpressWay Mobile and Remote Access – Scenario 1 CUCM Server Discovery

	Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
☐	COLCM9PUB.coluc.com	ccmadmin	On	COLCM9SUB1.coluc.com, COLCM9PUB.coluc.com	View/Edit

New | Delete | Select all | Unselect all | Refresh servers

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

Currently found Unified CM nodes

Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB.coluc.com	TCP	9.1.2	TCP: Active
COLCM9PUB.coluc.com	COLCM9SUB1.coluc.com	TCP	9.1.2	TCP: Active

When FQDN is returned shows ‘Active’ when xway can DNS resolve <hostname>@<domain> as configured in CCMADMIN

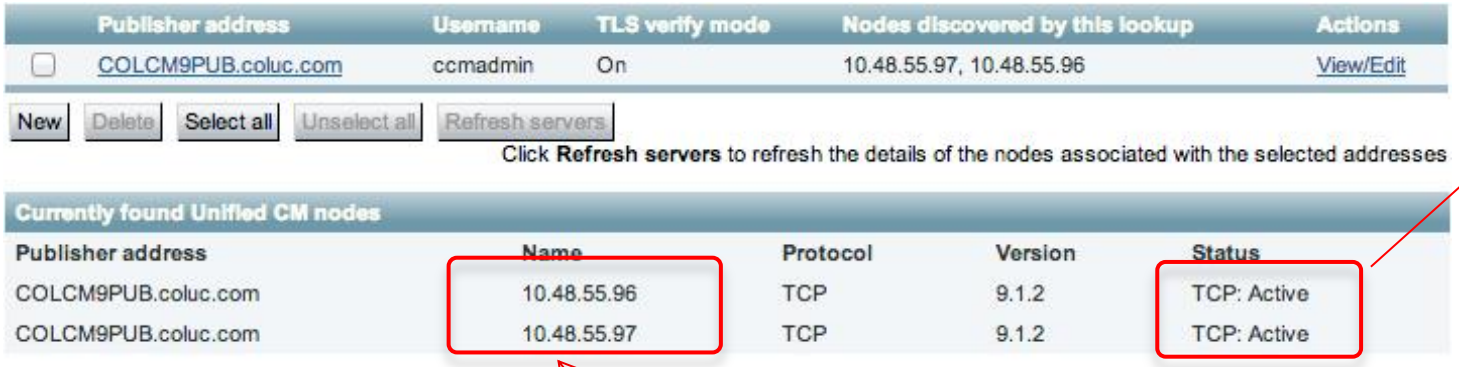
Here colcm9pub.coluc.com and colcm9sub1.coluc.com

Servers *(1 - 2 of 2)* **Rows per Page** 50

Find Servers where Host Name/IP Address begins with Find Clear Filter

	Host Name/IP Address	Description
☐	COLCM9PUB.coluc.com	COLCM9PUB
☐	COLCM9SUB1.coluc.com	COLCM9SUB1

ExpressWay Mobile and Remote Access – Scenario 1
CUCM Server Discovery



Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
COLCM9PUB.coluc.com	ccmadmin	On	10.48.55.97, 10.48.55.96	View/Edit

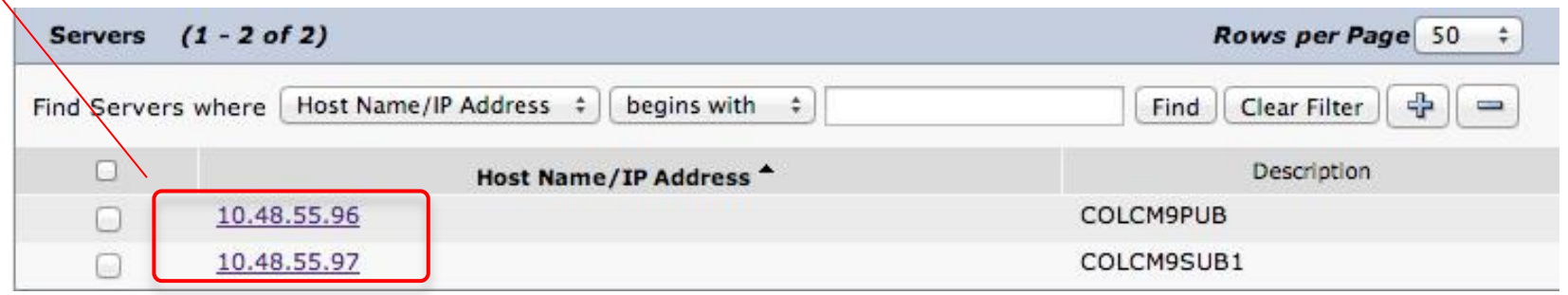
New | Delete | Select all | Unselect all | Refresh servers

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

Currently found Unified CM nodes

Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	10.48.55.96	TCP	9.1.2	TCP: Active
COLCM9PUB.coluc.com	10.48.55.97	TCP	9.1.2	TCP: Active

No DNS query is required as IP address is used.
Will always show Active



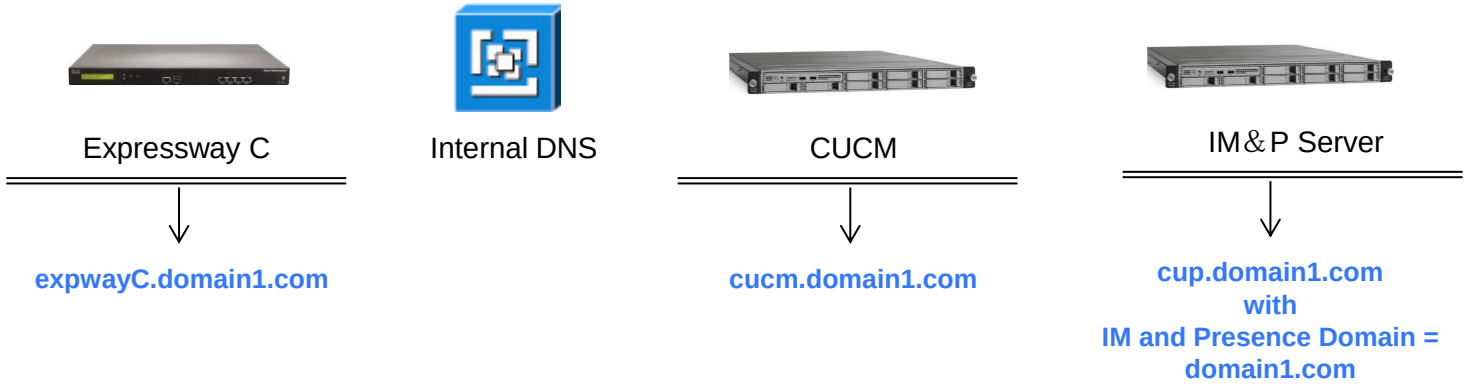
Servers *(1 - 2 of 2)* **Rows per Page** 50

Find Servers where Host Name/IP Address begins with Find Clear Filter

Host Name/IP Address	Description
10.48.55.96	COLCM9PUB
10.48.55.97	COLCM9SUB1

ExpressWay – Mobile and Remote Access
UC Server discovery

- Scenario 2
  - CUCM set to secure (mixed-mode)



ExpressWay – Mobile and Remote Access
UC Server discovery

- What does change when CUCM cluster is set to mixed mode?
  - Same steps need to be followed
  - Status will show ‘TLS/TCP’

	Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Actions
☐	COLCM9PUB.coluc.com	ccmadmin	On	COLCM9SUB1, COLCM9PUB	View/Edit

New | Delete | Select all | Unselect all | Refresh servers

Click **Refresh servers** to refresh the details of the nodes associated with the selected addresses

Currently found Unified CM nodes

Publisher address	Name	Protocol	Version	Status
COLCM9PUB.coluc.com	COLCM9PUB	TLS / TCP	9.1.2	TLS: Active, TCP: Active
COLCM9PUB.coluc.com	COLCM9SUB1	TLS / TCP	9.1.2	TLS: Active, TCP: Active

ExpressWay – Mobile and Remote Access
UC Server discovery

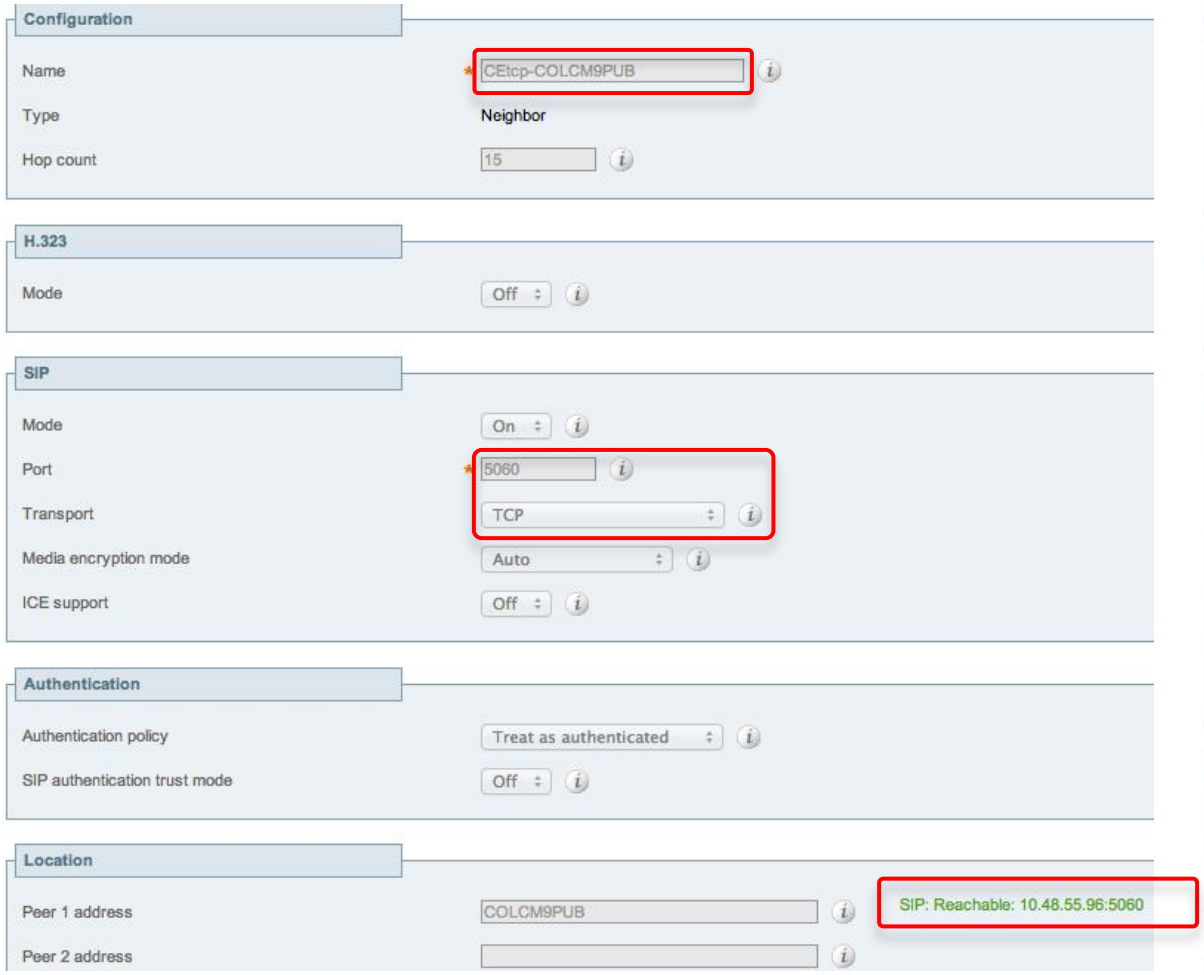
- TLS and TCP zone is auto-added per discovered node
  These are Non-configurable neighbor zones “CEtcp-<UCMName>” or/and “CEtls-<UCMName>”

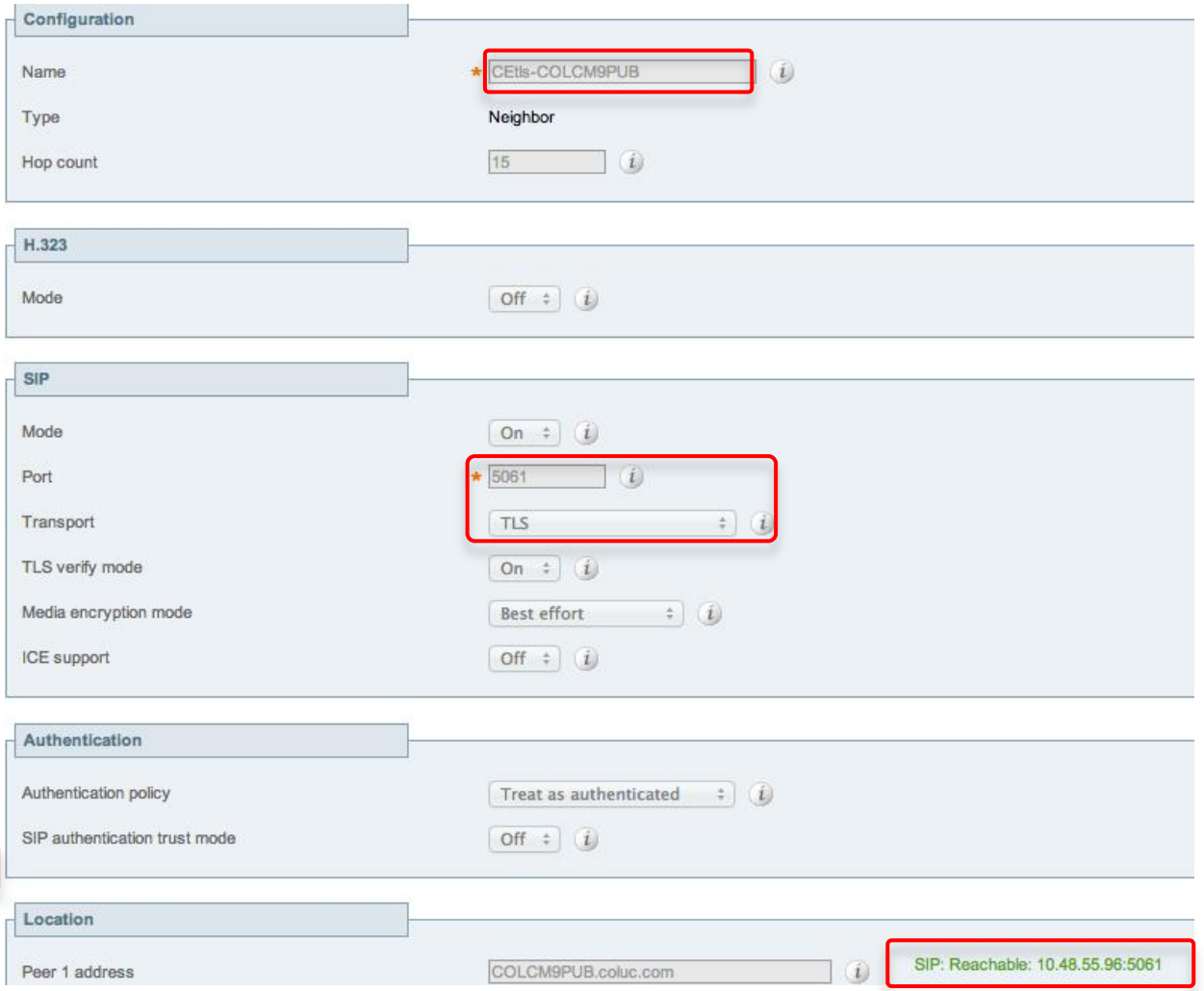
Zones

You are here: Configuration ▸ Zones

	Name	Type	Calls	Bandwidth used	H323 status	SIP status	Search rule status	Actions
	DefaultZone	Default zone	0	0 kbps	On	On		View/Edit
	CEtcp-COLCM9PUB	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View
	CEtcp-COLCM9SUB1	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View
	CEtls-COLCM9PUB	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View
	CEtls-COLCM9SUB1	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1	View
☐	TraversalZone	Traversal client	0	0 kbps	Off	Active	No search rules configured	View/Edit

ExpressWay – Mobile and Remote Access
UC Server discovery





ExpressWay – Mobile and Remote Access
UC Server discovery

- Search Rule on ExpressWay C is automatically added

Search rules

You are here: Configuration ▸ Dial plan ▸ Search rules

	Priority	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	State	Actions
	45	CEtcp-COLCM9PUB	SIP	Any	No	Alias pattern match	Prefix	COLCM9PUB;transport=TCP	Leave	Stop	CEtcp-COLCM9PUB	✔ Enabled	View
	45	CEtls-COLCM9PUB	SIP	Any	No	Alias pattern match	Prefix	COLCM9PUB;transport=TLS	Leave	Stop	CEtls-COLCM9PUB	✔ Enabled	View
	45	CEtcp-COLCM9SUB1	SIP	Any	No	Alias pattern match	Prefix	COLCM9SUB1;transport=TCP	Leave	Stop	CEtcp-COLCM9SUB1	✔ Enabled	View
	45	CEtls-COLCM9SUB1	SIP	Any	No	Alias pattern match	Prefix	COLCM9SUB1;transport=TLS	Leave	Stop	CEtls-COLCM9SUB1	✔ Enabled	View
☐	50	LocalZoneMatch	Any	Any	No	Any alias				Continue	LocalZone	✔ Enabled	View/Edit

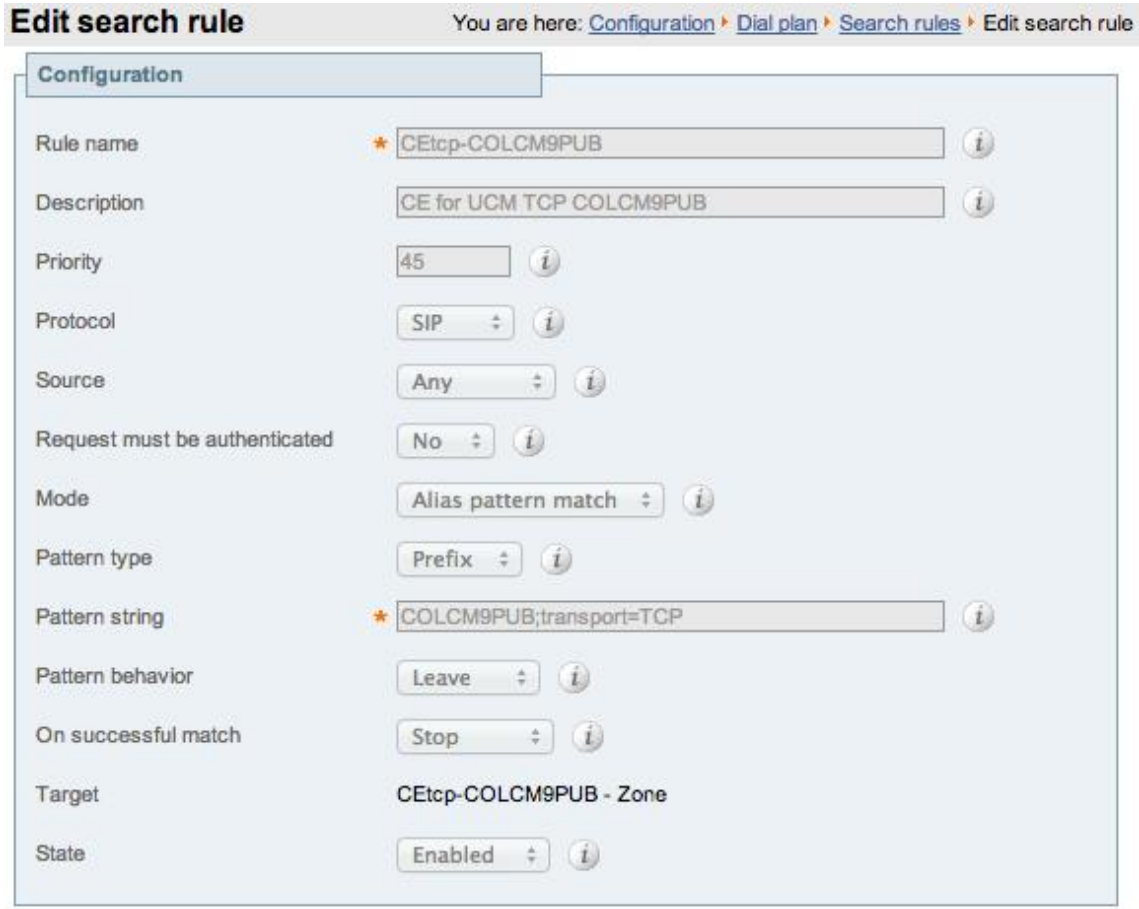
New | Delete | Enable | Disable | Select all | Unselect all

☐ Hide generated items

Search rules are applied in priority order, with 1 being the highest priority

ExpressWay – Mobile and Remote Access
UC Server discovery

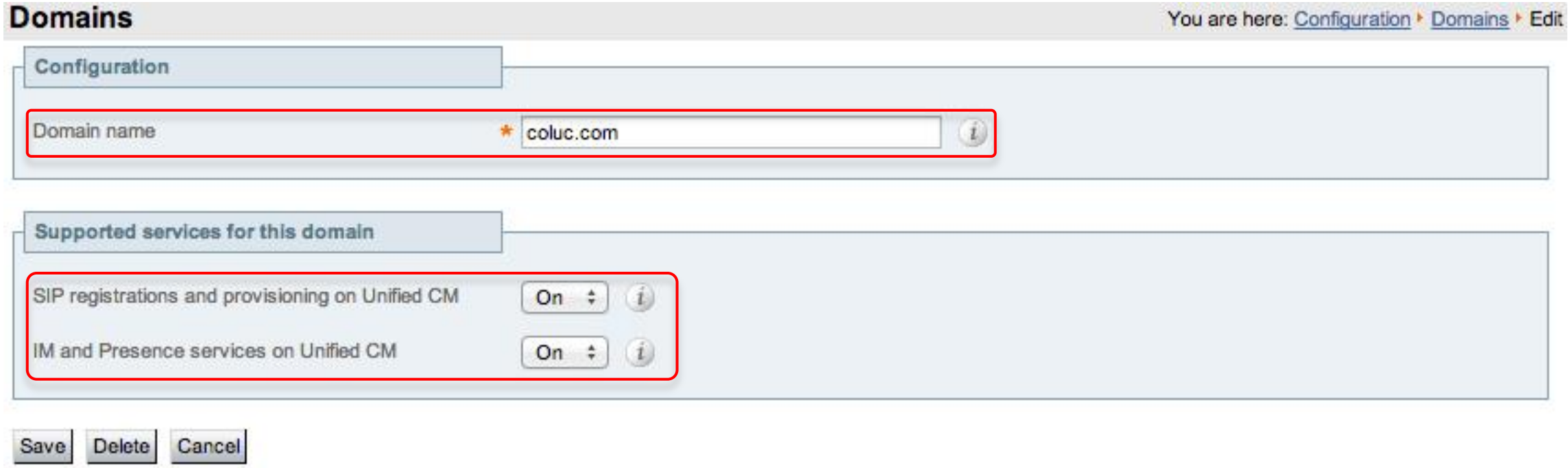
- Search Rules on none-configurable



DNS and Domain configuration

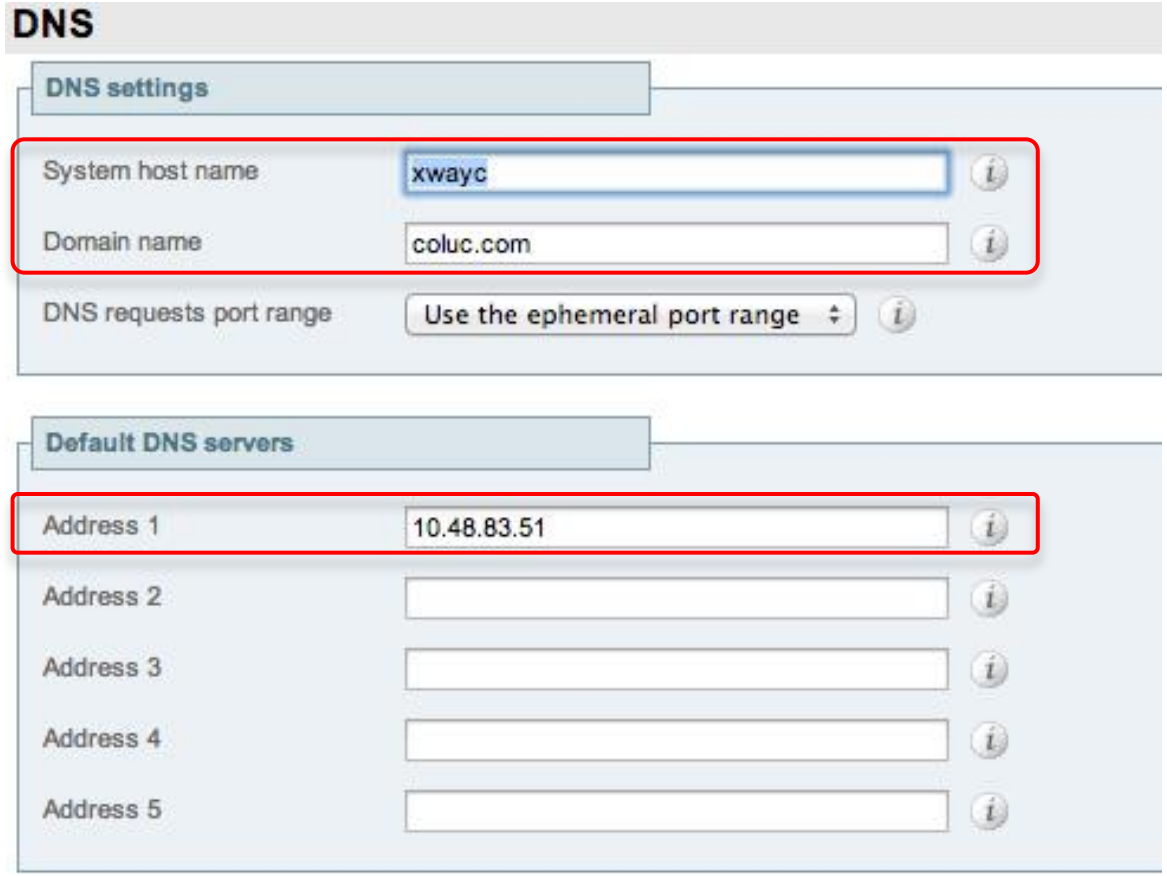
Domain Configuration
ExpressWay C – Domain Configuration

> Configurations > Domains



Domain Configuration
ExpressWay C & E – DNS Configuration

- System > DNS



Collaboration Edge Service Record (SRV)

- For a Jabber client to be able to log in successfully with MRA, a specific collaboration edge SRV record must be created and accessible externally. When a Jabber client is initially started, it makes DNS SRV queries:

- **_cisco-uds**: This SRV record is used in order to determine if a CUCM server is available.

- **_cuplogin**: This SRV record is used in order to determine if an IM&P server is available.

- **_collab-edge**: This SRV record is used in order to determine if MRA is available.

Client Service Discovery

- Service discovery enables clients and endpoints to automatically detect and locate service.
- The client/endpoint does query DNS servers to retrieve service (SRV) records that provide the location of servers.
- Clients/endpoints outside the internal network must be able to resolve '_collab-edge._tls.<domain>' SRV record which must point to the ExpressWay E server.
- Clients/endpoints but also ExpressWay C must be able to resolve '_cisco-uds._tcp.<domain>' SRV record which must point to the CUCM cluster.
- The external DNS may not resolve '_cisco-uds._tcp' SRV records
- The internal DNS may not resolve '_collab-edge._tls' SRV records

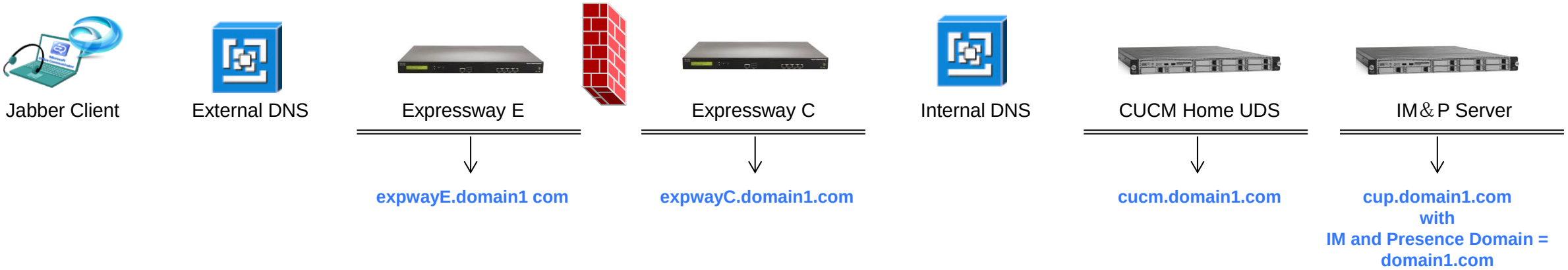
Client Service Discovery

- If the Jabber client is started and **does not** receive an SRV answer for **_cisco-uds** and **_cuplogin** and **does** receive an answer for **_collab-edge**, then it uses this answer to try to contact the Expressway-E listed in the SRV answer.

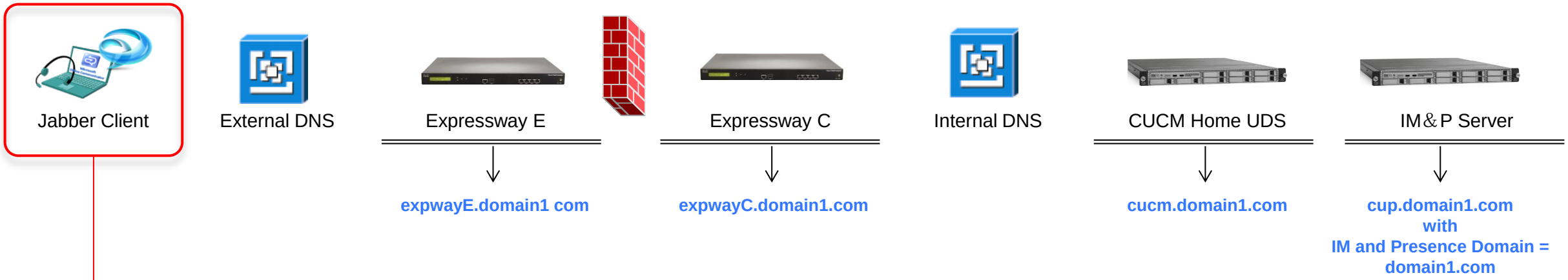
- The **_collab-edge** SRV record should point to the Fully Qualified Domain Name (FQDN) of Expressway-E with port **8443**. If the **_collab-edge** SRV is not created, or is not externally available, or if it is available, but port 8443 is not reachable, then the Jabber client fails to log in.

ExpressWay Mobile and Remote Access
Domain & DNS configuration

- Scenario
  - Flat domain structure
  - ExpressWay Servers : domain1.com
  - UC servers : domain1.com
  - IM&P domain : domain1.com



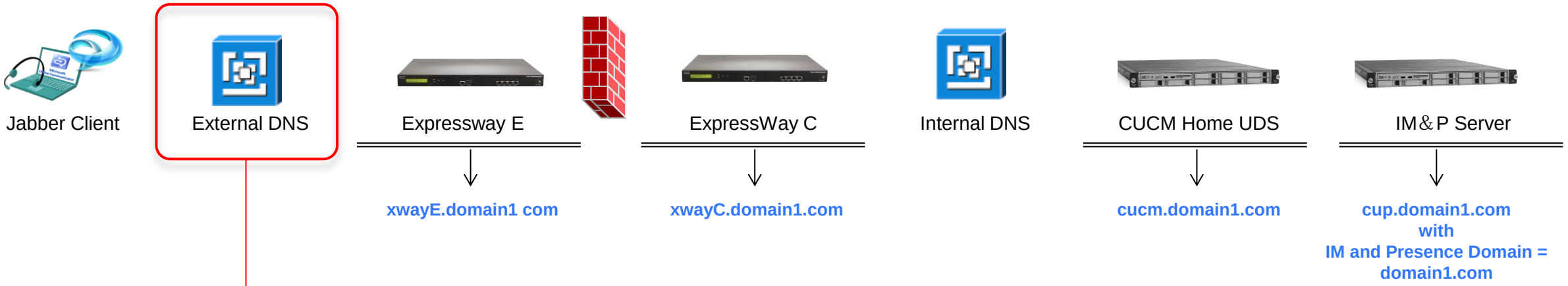
ExpressWay Mobile and Remote Access Domain & DNS configuration



Question : How do I login?

Answer : With <userid>@domain1.com

ExpressWay Mobile and Remote Access Domain & DNS configuration

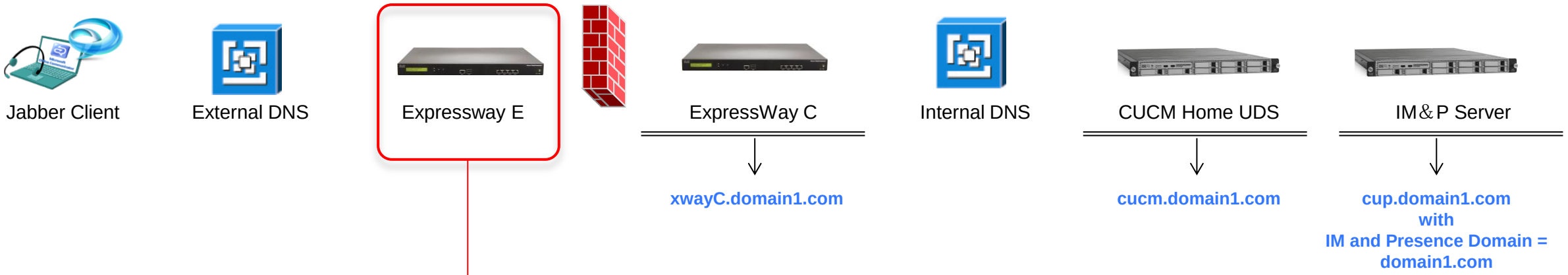


Question: How is my external DNS configured?

Answer:

Entry	Resolves to
SRV record '_collab-edge._tls.domain1.com'	xwayE.domain1.com port 8443
A record 'xwayE.domain1.com'	External IP address ExpressWay E

ExpressWay Mobile and Remote Access Domain & DNS configuration



Question: How is my ExpressWay E configured?

Answer:

> System > DNS >

- System host name ‘xwayE’
- Domain name ‘domain1.com’

ExpressWay Mobile and Remote Access Domain & DNS configuration

Question: How is my ExpressWay C configured?
Answer:

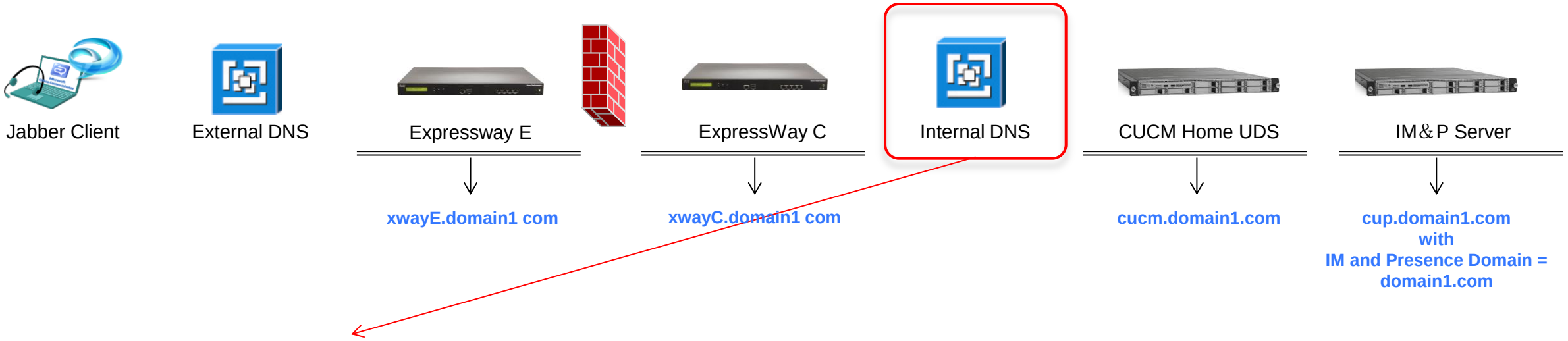
> System > DNS >

- System host name ‘xwayC’
- Domain name ‘domain1.com’

> Configuration > Domains >

- Domain ‘domain1.com’ enabled for ‘UCM registrations’ and ‘IM and Presence’

ExpressWay Mobile and Remote Access Domain & DNS configuration

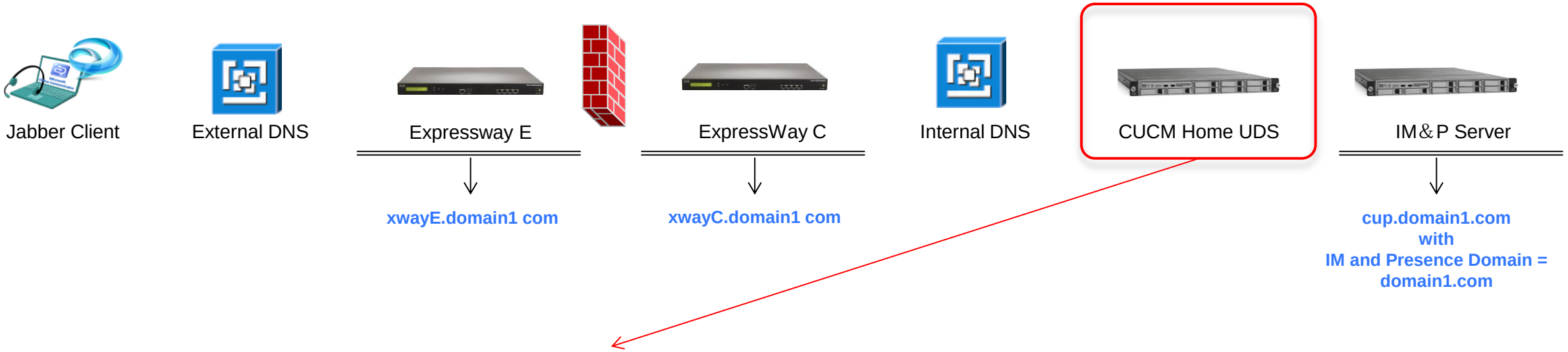


Question: How is my Internal DNS configured?

Answer:

Entry	Resolves to
SRV record '_cisco-uds._tcp.domain1.com'	cucm.domain1.com port 8443
A record 'cucm.domain1.com'	IP address of CUCM
SRV record '_cuplogin._tcp.domain1.com	cup.domain1.com port 8443
A record 'cup.domain1.com'	IP address of CUP

ExpressWay Mobile and Remote Access Domain & DNS configuration



Question: How is my CUCM configured?

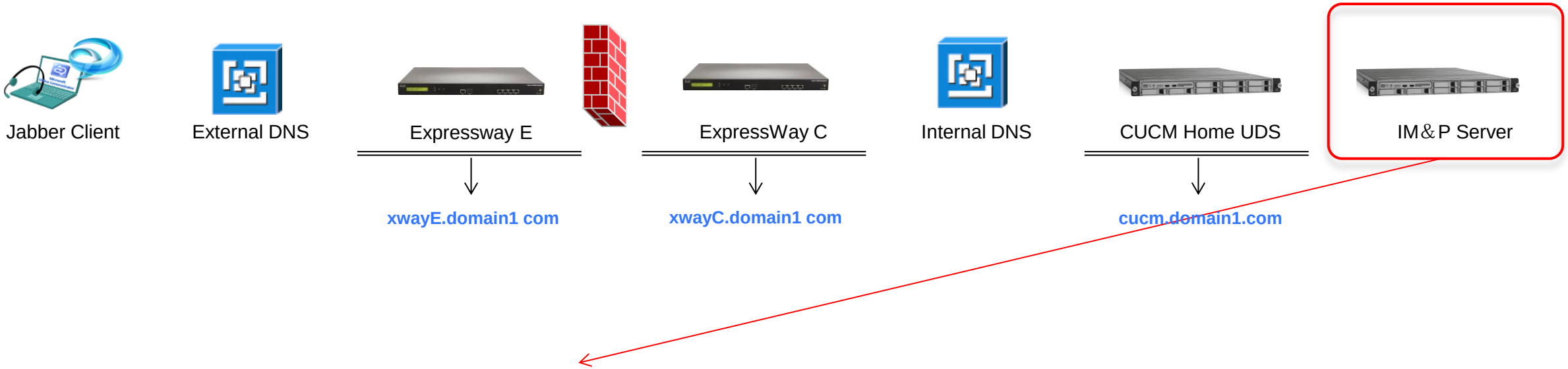
Answer:

> CCMADMIN > System > Server

- Server with hostname ‘cucm’

> CLI ‘set network domain ‘domain1.com’

ExpressWay Mobile and Remote Access
Domain & DNS configuration



Question: How is my CUP configured?

Answer:

> CUPAdmin > Clustertopology

- Node configuration with ‘cup.domain1.com
- IM and Presence Domain with ‘domain1.com’(*)

(*) Only 1 is supported

ExpressWay Mobile and Remote Access
ExpressWay or UC Server Domain not configured

- ExpressWay or UC server domain not added or not enabled for Unified Communications
- Jabber login will fail – Cannot communicate with the server
- Diagnostic logs will show

HTTPMSG:|GET
https:///Y29sdWMuY29t/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin
HTTP/1.1Authorization: xxxxxHost: xwaye.coluc.com:8443
Accept: */*User-Agent: Jabber-Win-345

HTTPMSG:|HTTP/1.1 403 Forbidden
Date:
Mon, 17 Mar 2014 16:07:20 GMT
Connection: closeServer:
CE_EContent-Length: 0|

Decodes to ‘coluc.com’

ExpressWay Mobile and Remote Access IM&P Domain not configured (UC Domain)

- IM&P domain not added or not enabled for IM&P
- Jabber login will fail – Cannot communicate with the server
- Diagnostic logs will show

  xwaye XCP_JABBERD[12144]: UTCTime="2014-03-14 14:30:25,310" ThreadID="140582990952192" Module="Jabber" Level="INFO " CodeLocation="deliver.c:1492" Detail="bouncing a packet to 'domain3.com" from 'cm-1_jsmcp-1.xwaye-domain1.com'"

  xwaye XCP_CM[12513]: UTCTime="2014-03-14 14:30:25,310" ThreadID="140004551300864" Module="cm-1.xwaye-domain1.com" Level="INFO " CodeLocation="SASLManager.cpp:198" Detail="Failed to query auth component for SASL mechanisms"

Serviceability ExpressWay

ExpressWay C “Unified Communications” status

- Status > Unified Communications

Unified Communications — You are here: Status › Unified Communications

Unified Communications (last updated: 18:23:24 UTC)	
Unified Communications status	Enabled
Unified Communications services	Active
IM and Presence servers	1
Unified CM servers	2
Activity	
Current provisioned sessions	2
Total provisioning requests since last restart	2
Total provisioned sessions since last restart	2
Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0

Domains		
Name	**Services**	**Associated zones**
coluc.com	Unified CM registrations, IM and Presence	TraversalZone

Zones	
Name	**SIP status**
TraversalZone	Active

Advanced status information

View provisioning sessions

View ssh tunnel status

ExpressWay C “Unified Communications” status

- Unified Communications > View provisioned sessions

Unified Communications proxy requests

You are here: Status ▸ Unified Communications ▸ Unified Communications proxy requests

Records: 5 Page 1 of 1

Username	Device	User agent	Unified CM server	Expire time
ewayj	10.10.1.7	Jabber-Win-293	colcm9pub	2014-03-26 02:22:48
ewayj	10.10.1.7	Jabber-Win-969	colcm9pub	2014-03-26 00:44:10
ewayj	10.10.1.7	Jabber-Win-101	colcm9pub	2014-03-26 00:45:50
ewayj	10.10.1.7	Jabber-Win-293	colcm9pub	2014-03-26 02:22:49
ewayj	10.10.1.7	Jabber-Win-101	colcm9pub	2014-03-26 00:45:49

Related tasks

View Unified CM servers

ExpressWay E – “Unified Communications” status

- Status > Unified Communications

Unified Communications — You are here: Status ▸ Unified Communications

Unified Communications (last updated: 18:24:41 UTC)		
Unified Communications status	Enabled	
Unified Communications services	Active	
Activity		
Unified CM calls: Current video	0	
Unified CM calls: Current audio (SIP)	0	
Domains		
Name	**Services**	**Associated zones**
coluc.com	Unified CM registrations, IM and Presence	TraversalZone
Zones		
Name	**SIP status**	
TraversalZone (xwayc.coluc.com)	Active	

Advanced status information

View ssh tunnel status

ExpressWay C – “Call Status”

- Status > Calls > Calls (active) or History

Call status

You are here: Status ▸ Calls ▸ Calls

Records: 1 Page 1 of 1

	Start time ▲	Duration	Source	Destination	Type	Protocol	Peer	Actions
☐	2014-03-25 18:27:08	1 minute 56 seconds	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	Traversal	Multiple components	This system	View

Disconnect | Select all | Unselect all

Call status

You are here: Status ▸ Calls ▸ Calls ▸ View

Status	
Status	Connected
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Box-unique call serial number	4b3abe17-358f-4f57-a757-ff9eeed39ee1
Source alias	sip:5000@COLCM9PUB
Destination alias	sip:9011@COLCM9PUB
Start time	2014-03-25 18:27:08
Duration	2 minutes 31 seconds

Call components

Local call serial number	Source alias	Destination alias	Protocol	Type
a5988187-374e-424c-80fc-a7df8cf101d3	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway
daa60af9-a970-483a-99fc-f90f4dc21d19	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Encryption B2BUA
9a4db343-a8fd-43ad-9476-b93af9fc635b	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway

Disconnect

ExpressWay C – Traversal Call

Call details

You are here: Status ▸ Calls ▸ Calls ▸ Call details

Call information	
State	Connected
Start time	2014-03-25 18:27:08
Duration	5 minutes 39 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	a5988187-374e-424c-80fc-a7df8cf101d3
Type	Video
Bandwidth	
Requested	4000 kbps
Allocated	64 kbps
Route	TraversalZone -> Zone001ToTraversalSZ -> TraversalSubZone -> Zone004ToTraversalSZ -> CEtls-COLCM9PUB
Leg 1	
Bandwidth node	TraversalZone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.48.55.99:7001
Transport	TLS
Encryption type	None
Leg 2	
Bandwidth node	
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	Not set
Transport	SIP Transport Protocol Undefined
Leg 3	
Bandwidth node	CEtls-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.96:5061
Transport	TLS
Leg 4	
Bandwidth node	CEtls-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.98:5071
Transport	TLS
Encryption type	AES

Session 1	
Status	Searching
Media routed	False
Call routed	False
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	0 kbps
Bandwidth requested	0 kbps
Session 2	
Status	Replaced
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 3
Bandwidth allocated	0 kbps
Bandwidth requested	0 kbps
Session 3	
Status	Connected
Media routed	False
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 4
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	TraversalZone -> Zone001ToTraversalSZ -> TraversalSubZone -> Zone004ToTraversalSZ -> CEtls-COLCM9PUB

- ExpressWay C B2BUA Call

- ExpressWay C – CUCM Call

Call details

You are here: Status ▸ Calls ▸ Calls ▸ Call details

Call information	
State	Connected
Start time	2014-03-25 18:27:08
Duration	7 minutes 16 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	9a4db343-a8fd-43ad-9476-b93af9fc635b
Type	Video
Leg 1	
Bandwidth node	Default zone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.48.55.98:5073
Transport	TLS
Encryption type	None
Leg 2	
Bandwidth node	CEtls-COLCM9PUB
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.96:5061
Transport	TLS
Encryption type	None
Session 1	
Status	Connected
Media routed	False
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2

ExpressWay E – “Call Status”

Call status

You are here: Status ▸ Calls ▸ Calls

Records: 1 Page 1 of 1

	Start time ▲	Duration	Source	Destination	Type	Protocol	Peer	Actions
☐	2014-03-25 18:27:08	9 minutes 26 seconds	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	Traversal	SIP <-> SIP	This system	View

Disconnect | Select all | Unselect all

Call status

You are here: Status ▸ Calls ▸ Calls ▸

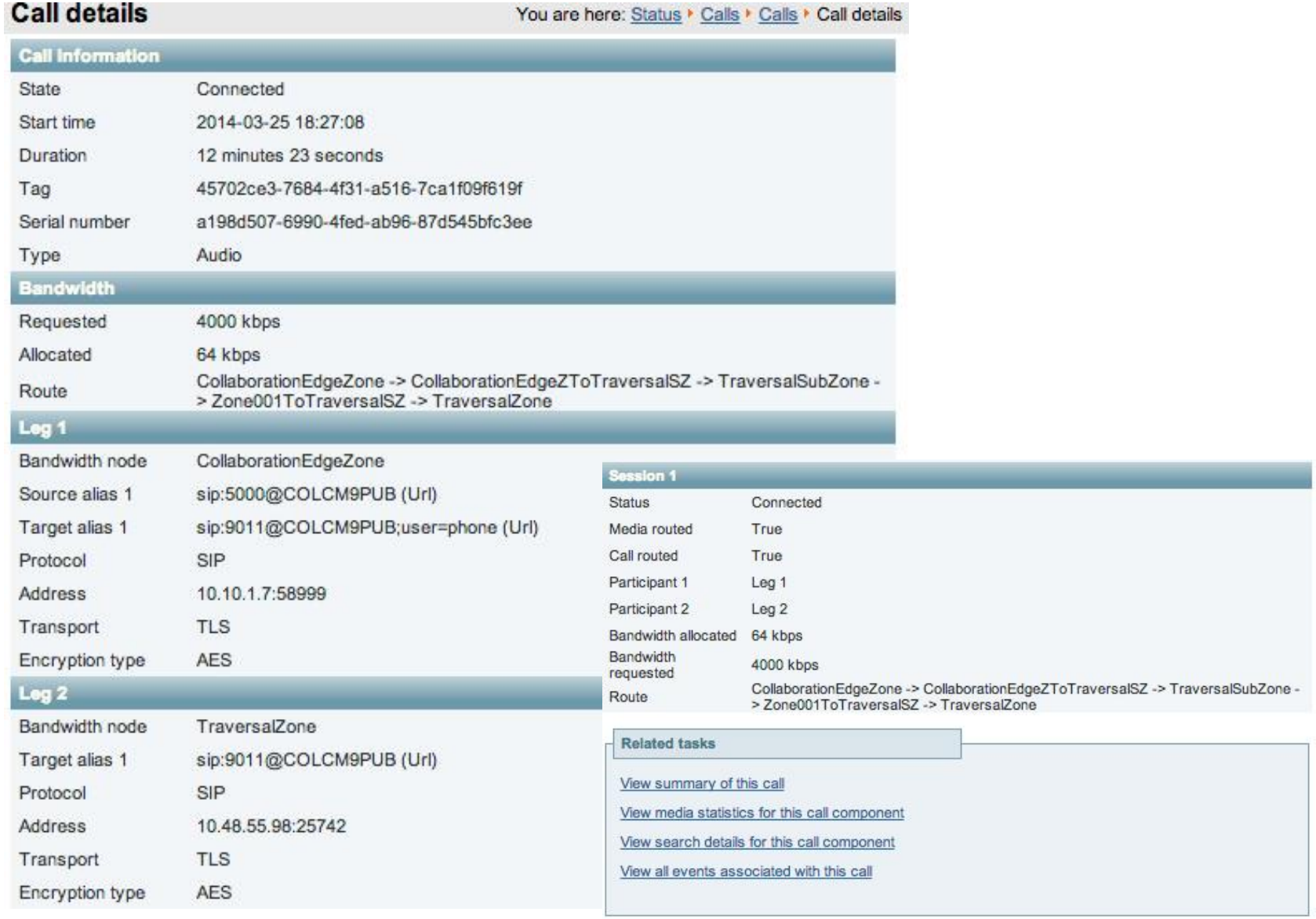
Status	
Status	Connected
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Box-unique call serial number	3012e784-b45d-4a9a-b2f0-c4d1988fc5d1
Source alias	sip:5000@COLCM9PUB
Destination alias	sip:9011@COLCM9PUB
Start time	2014-03-25 18:27:08
Duration	9 minutes 54 seconds

Call components

Local call serial number	Source alias	Destination alias	Protocol	Type
a198d507-6990-4fed-ab96-87d545bfc3ee	sip:5000@COLCM9PUB	sip:9011@COLCM9PUB	SIP <-> SIP	Expressway

Disconnect

- ExpressWay E Inbound Call



Call details

You are here: Status ▸ Calls ▸ Calls ▸ Call details

Call information

State	Connected
Start time	2014-03-25 18:27:08
Duration	12 minutes 23 seconds
Tag	45702ce3-7684-4f31-a516-7ca1f09f619f
Serial number	a198d507-6990-4fed-ab96-87d545bfc3ee
Type	Audio

Bandwidth

Requested	4000 kbps
Allocated	64 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone

Leg 1

Bandwidth node	CollaborationEdgeZone
Source alias 1	sip:5000@COLCM9PUB (Url)
Target alias 1	sip:9011@COLCM9PUB;user=phone (Url)
Protocol	SIP
Address	10.10.1.7:58999
Transport	TLS
Encryption type	AES

Leg 2

Bandwidth node	TraversalZone
Target alias 1	sip:9011@COLCM9PUB (Url)
Protocol	SIP
Address	10.48.55.98:25742
Transport	TLS
Encryption type	AES

Session 1

Status	Connected
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone

Related tasks

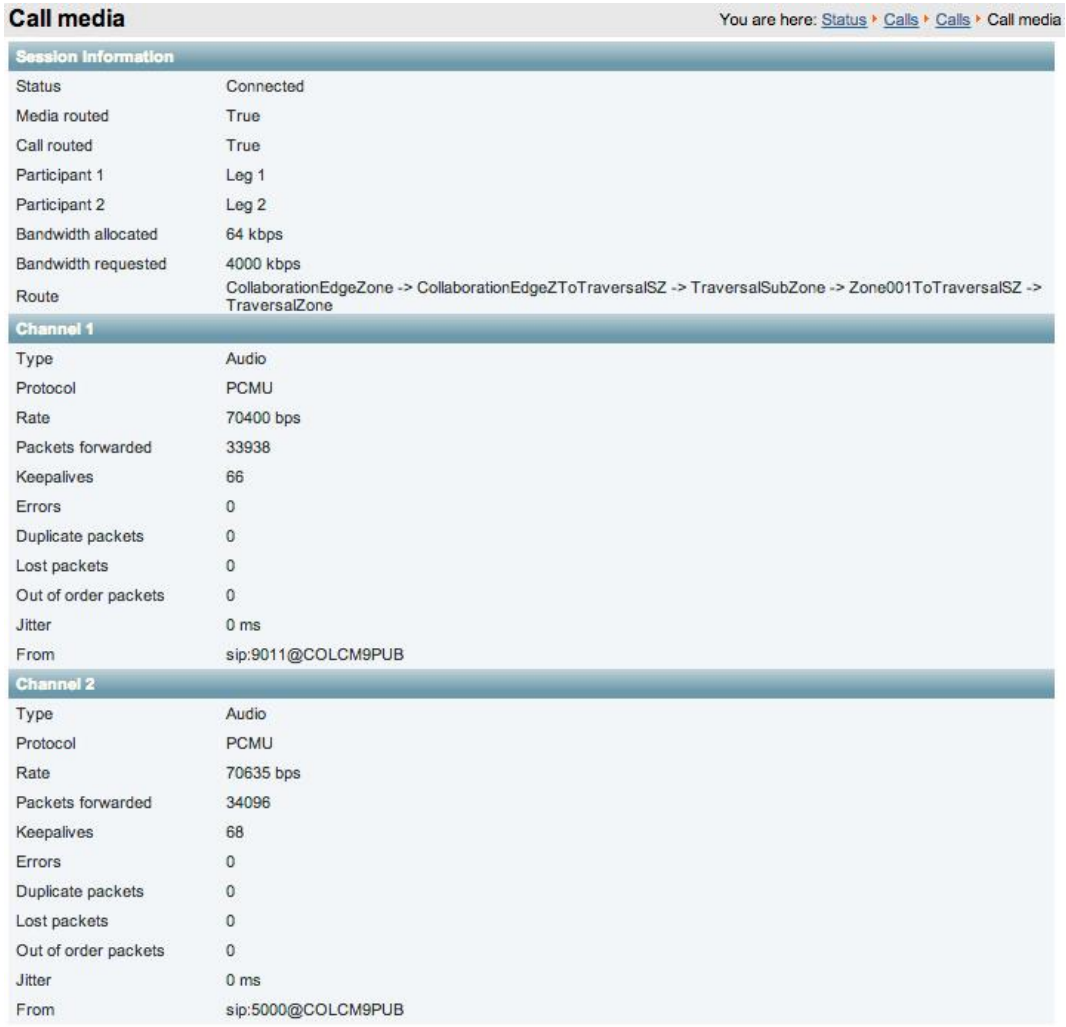
View summary of this call

View media statistics for this call component

View search details for this call component

View all events associated with this call

- Inbound Call Media Statistics



Call media

You are here: Status ▸ Calls ▸ Calls ▸ Call media

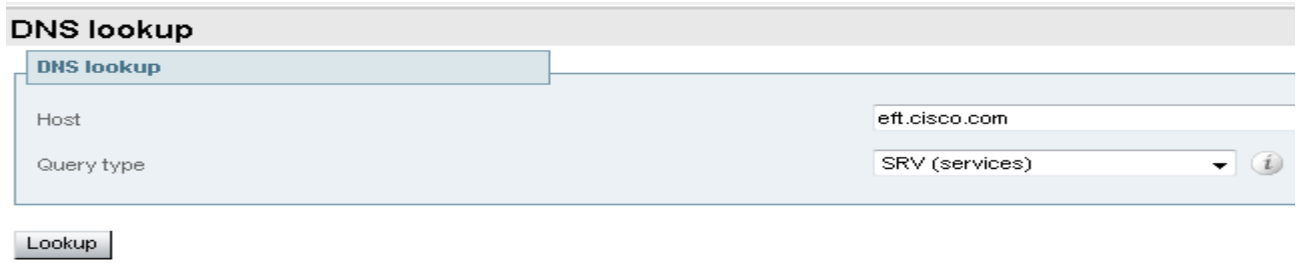
Session information	
Status	Connected
Media routed	True
Call routed	True
Participant 1	Leg 1
Participant 2	Leg 2
Bandwidth allocated	64 kbps
Bandwidth requested	4000 kbps
Route	CollaborationEdgeZone -> CollaborationEdgeZToTraversalSZ -> TraversalSubZone -> Zone001ToTraversalSZ -> TraversalZone
Channel 1	
Type	Audio
Protocol	PCMU
Rate	70400 bps
Packets forwarded	33938
Keepalives	66
Errors	0
Duplicate packets	0
Lost packets	0
Out of order packets	0
Jitter	0 ms
From	sip:9011@COLCM9PUB
Channel 2	
Type	Audio
Protocol	PCMU
Rate	70635 bps
Packets forwarded	34096
Keepalives	68
Errors	0
Duplicate packets	0
Lost packets	0
Out of order packets	0
Jitter	0 ms
From	sip:5000@COLCM9PUB

ExpressWay Tools

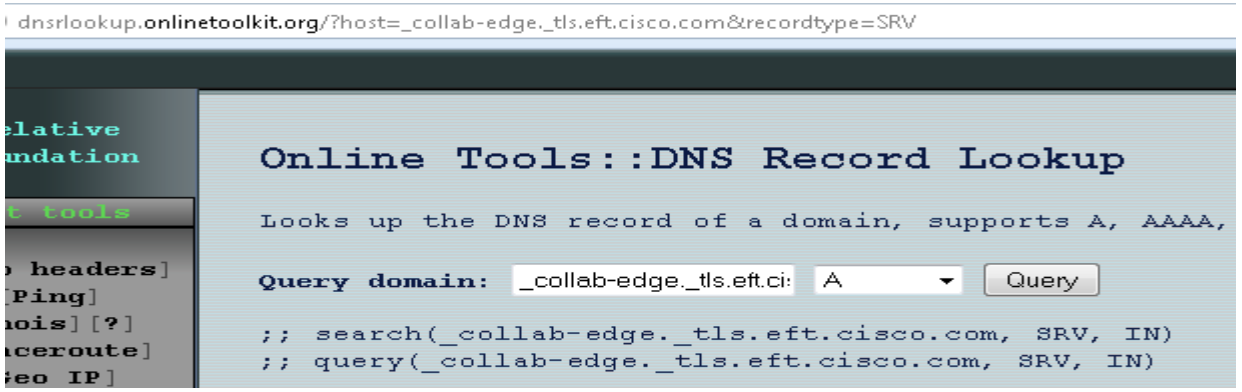
- Maintenance > Tools > Network Utilities
  Ping
  DNS lookup (also flush dns cache from DNS configuration)
  TraceRoute
  TracePath

DNS Lookup

- > Maintenance > Tools > Network Utilities > DNS Lookup (for internal DNS)

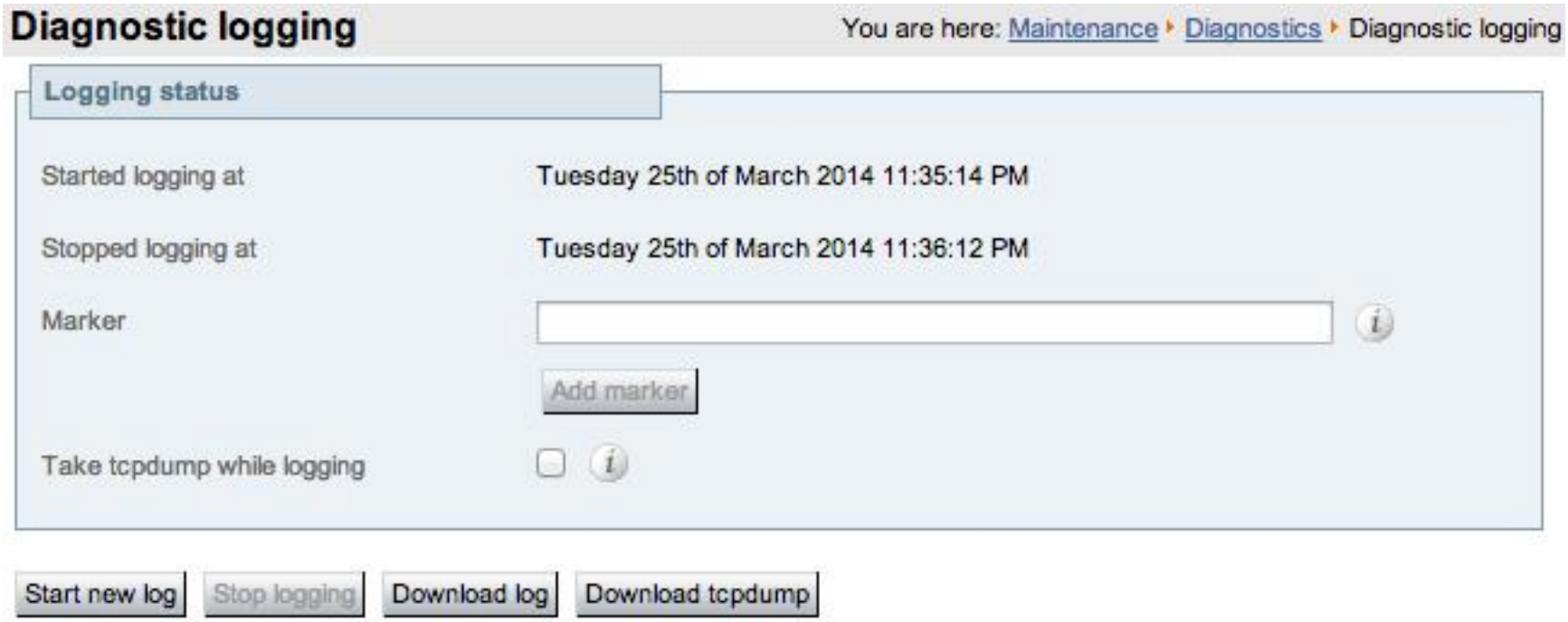


- Online Tools (for external) e.g http://dnsrlookup.onlinetoolkit.org/



ExpressWay Diagnostic Logs

- Maintenance > Diagnostics > Diagnostic Logging



(When using dual NIC will take TCPdump on internal interface, when required from external need to SSH into ExpressWay (root) and run e.g “tcpdump -s 0 –w -i eth1 /tmp/trace-1.pcap” and use wincp to transfer)

Jabber Registration Walk Through

Jabber pre-requirements

- Jabber 9.6 (Win/iOS) requires configuration key in **jabber-config.xml** to enable Mobile Remote Access:

  </Policies>
  <RemoteAccess>ON</RemoteAccess>
  </Policies>

- For local testing purposes, user can set the RemoteAccess configuration key on their device editing **jabberLocalConfig.xml** (J4Win)

  <Jabber>
  <userConfig name="remoteaccess" value="ON"/>
  </Jabber>

→ In the officially supported version of Jabber (9.7) Mobile and Remote Access will be enabled by default

Jabber URL transform

- Jabber transforms original Url: **http://colcm9pub:6970/CSFxwayj.cnf.xml**
- Base Url with appended Edge domain: coluc.com/
- Base Url with appended protocol: coluc.com/http/
- Base Url with appended host: coluc.com/http/colcm9pub
- Base Url before encoding: **coluc.com/http/colcm9pub/6970**
- Encoded Base64 Url: **Y29sdWMuY29tL2h0dHAvY29sY205cHViLzY5NzA=**
- Transformed Url:

https://xwaye.coluc.com:8443/Y29sdWMuY29tL2h0dHAvY29sY205cHViLzY5NzA=/CSFxwayj.cnf.xml

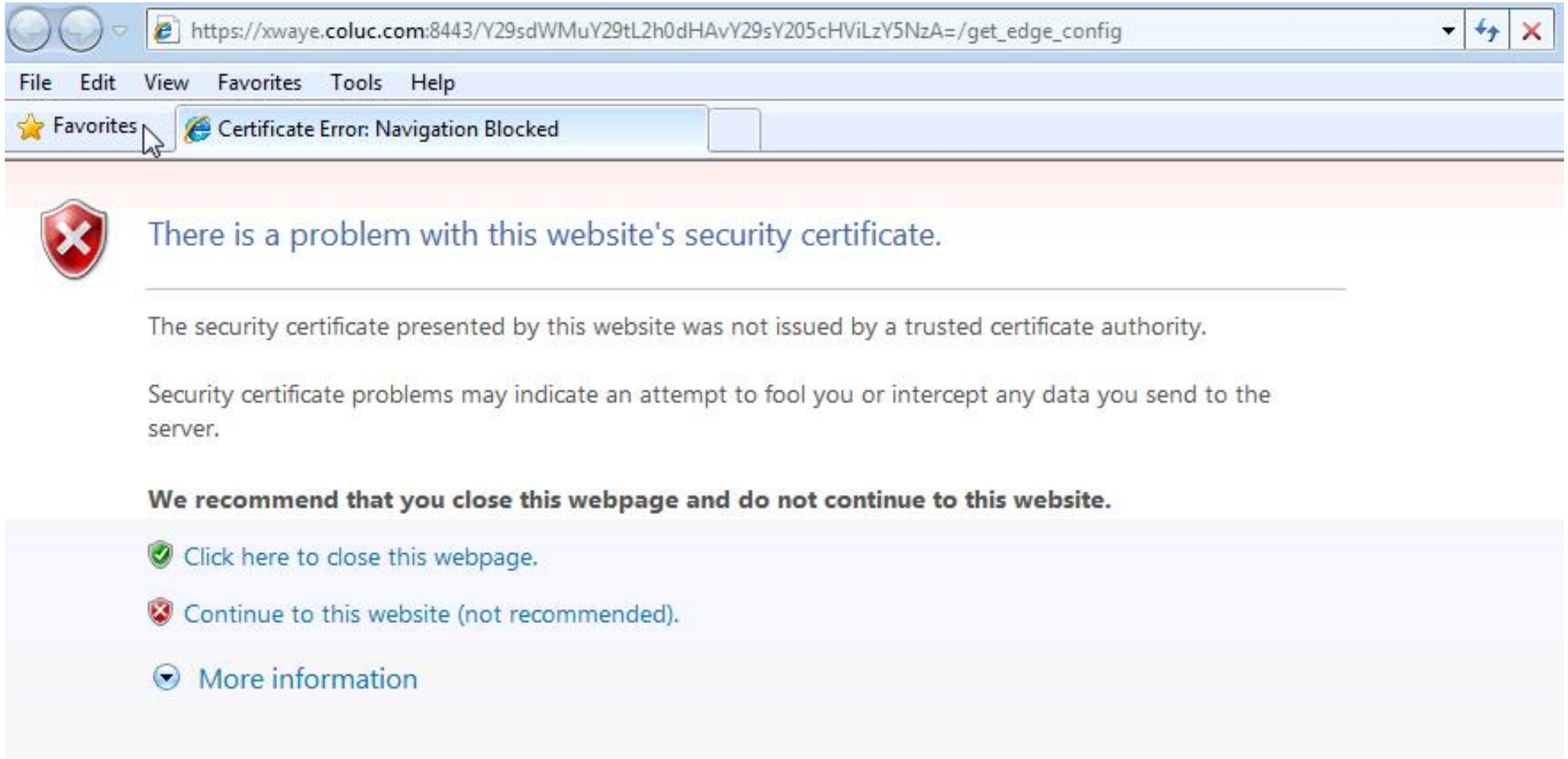
Jabber URL Transfer

- A good way to verify that the basic MRA components are in place is to run the first HTTP request Jabber would do.
- To do this verification, open a browser and enter the following URL to verify that the HTTP Reverse proxy is working, and that the ExpressWay-C can discover the DNS.

  https://xwaye.coluc.com:8443/**Y29sdWMuY29tL2h0dHAvY29sY205cHViLzY5NzA=**/get_edge_config
- Use a CUCM User credentials when prompted by the browser
- Use http://www.base64decode.org/ to encode/decode

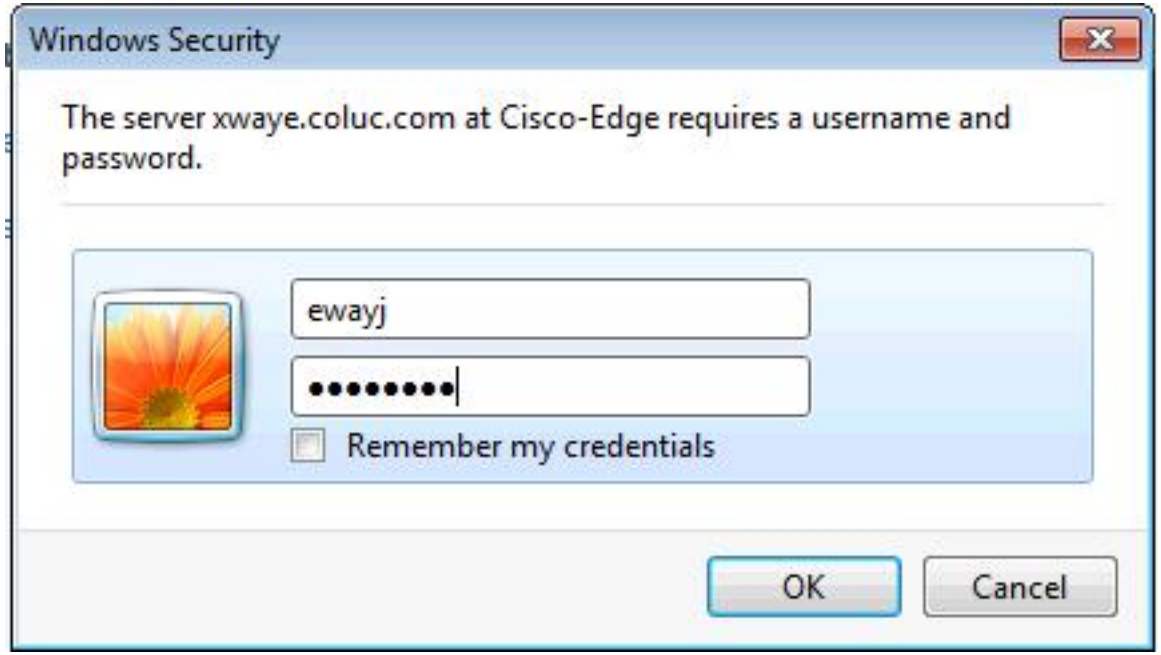
Jabber URL Transform

- Expressway E certificate not trusted (Jabber client will prompt same)



Jabber URL Transform

- Provide CCM user credentials



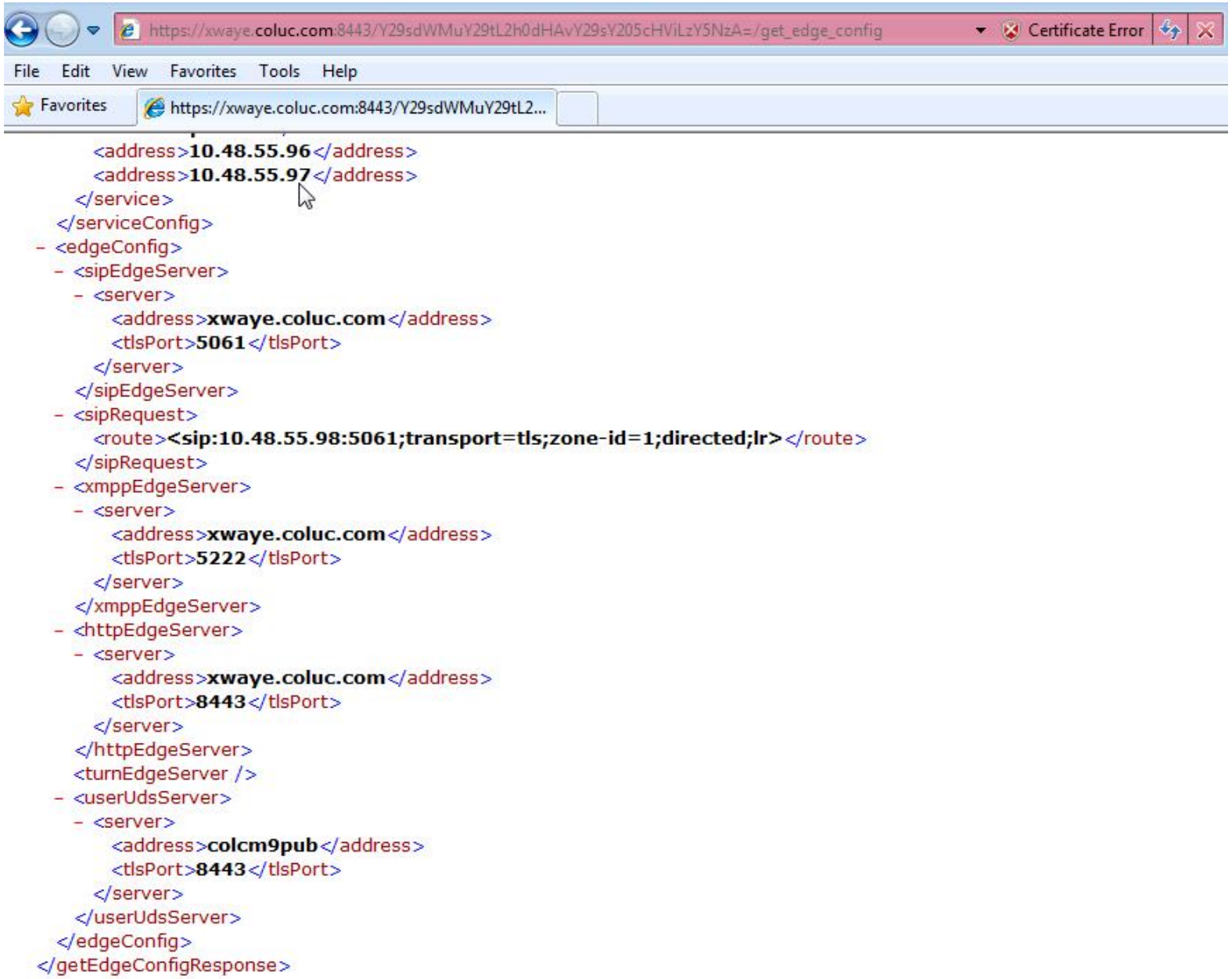
Jabber URL Transform

- Service Config


```
<?xml version="1.0" encoding="UTF-8" ?>
- <getEdgeConfigResponse version="1.0">
  - <serviceConfig>
    - <service>
        <name>_cisco-phone-tftp</name>
      - <server>
          <priority>0</priority>
          <weight>0</weight>
          <port>8443</port>
          <address>colcm9pub.coluc.com</address>
        </server>
      </service>
    - <service>
        <name>_cuplogin</name>
        <error>NameError</error>
      </service>
    - <service>
        <name>_cisco-uds</name>
      - <server>
          <priority>0</priority>
          <weight>0</weight>
          <port>8443</port>
          <address>colcm9pub.coluc.com</address>
        </server>
      </service>
    - <service>
        <name>tftpServer</name>
        <address>10.48.55.96</address>
        <address>10.48.55.97</address>
      </service>
  </serviceConfig>
```

Jabber URL Transform

- Edge Configuration



Common Issue 1

Softphone is Not Able to Register, SIP/2.0 405 Method Not Allowed

A diagnostic log from Expressway-C shows a **SIP/2.0 405 Method Not Allowed** message in response to the Registration request sent by the Jabber client. This is likely due to an existing Session Initiation Protocol (SIP) trunk between Expressway-C and CUCM using port 5060/5061.

SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0

In order to correct this issue, change the SIP port on the SIP Trunk Security Profile that is applied to the existing SIP trunk configured in CUCM and the Expressway-C neighbor zone for CUCM to a different port such as 5065. This is explained further in the MRA Deployment Guide on Page 39.

Configuration Summary

CUCM:

1.Create a new SIP Trunk security profile with a listening port other than 5060 (5065).
2.Create a SIP Trunk associated to the SIP Trunk Security Profile and destination set to the Expressway-C IP address, port 5060.

Expressway-C:

1.Create a neighbor zone to CUCM(s) with a target port other than 5060 (5065) to match the CUCM configuration.
2.In Expressway-C **Settings > Protocols > SIP**, make sure Expressway-C still listens on 5060 for SIP.

Common Issue 2

Unable to Log In Because of an Existing WebEx Connect Subscription

Jabber for Windows logs show this:

2014-11-22 19:55:39,122 INFO [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)] [service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server: http://loginp.webexconnect.com;
Url: http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com';;;.2014-11-22 19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)] [service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] - Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122 DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)] [service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_ lookup_url : http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com2014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)] [ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url] value : [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com]2014-11-22 19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)] [TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url] skipLocal : [0] value: [http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com] success: [true] configStoreName: [LocalFileConfigStore]

The login attempts are directed to WebEx Connect.

For a permanent resolution, you must contact WebEx in order to have the site decommissioned.

Workaround:

In the short-term, you can utilize one of these two options to exclude it from the lookup.

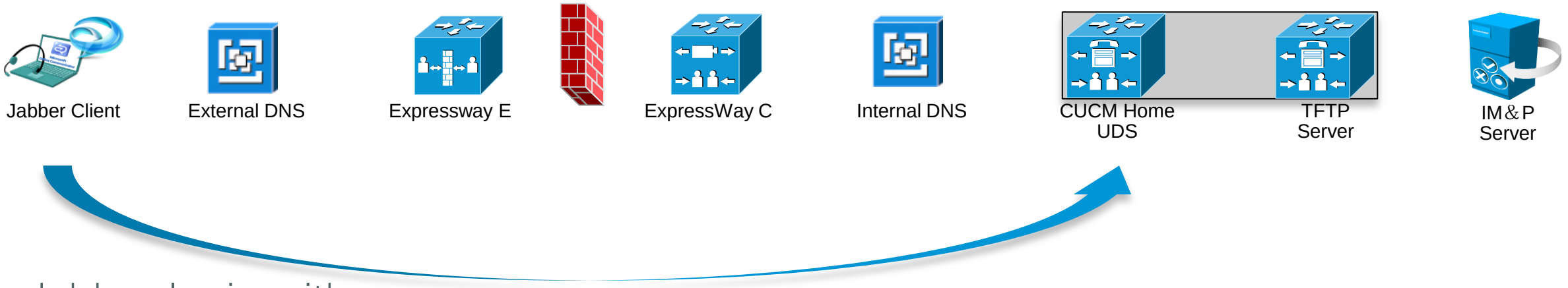
•Add this parameter to the jabber-config.xml. Then upload the jabber-config.xml file to the TFTP server on CUCM. It requires that the client logs in internally first.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

•From an application perspective, run this: **msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX**

Jabber Registration – Walk Trough

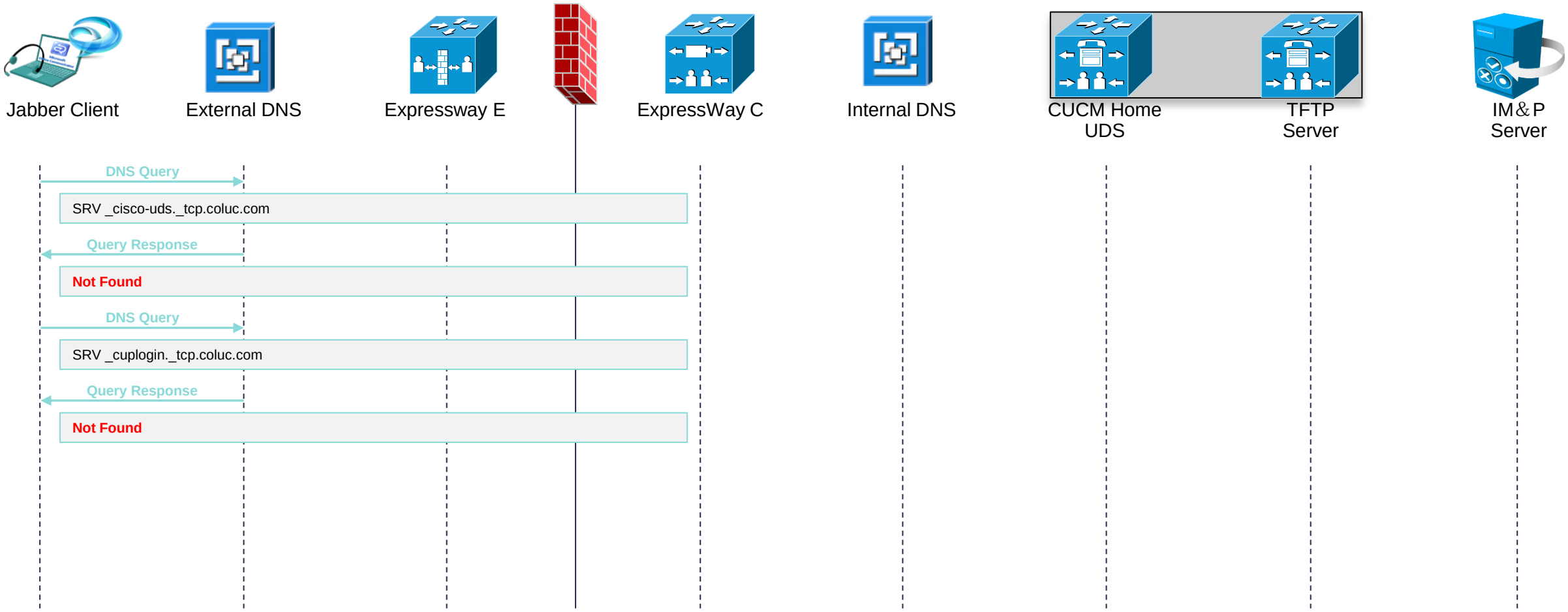
- Register Jabber client on UCM via MRA
  Expected signaling flow for Jabber Client logon and registration on simple IM&P based deployment



Jabber login with
xwayj@coluc.com

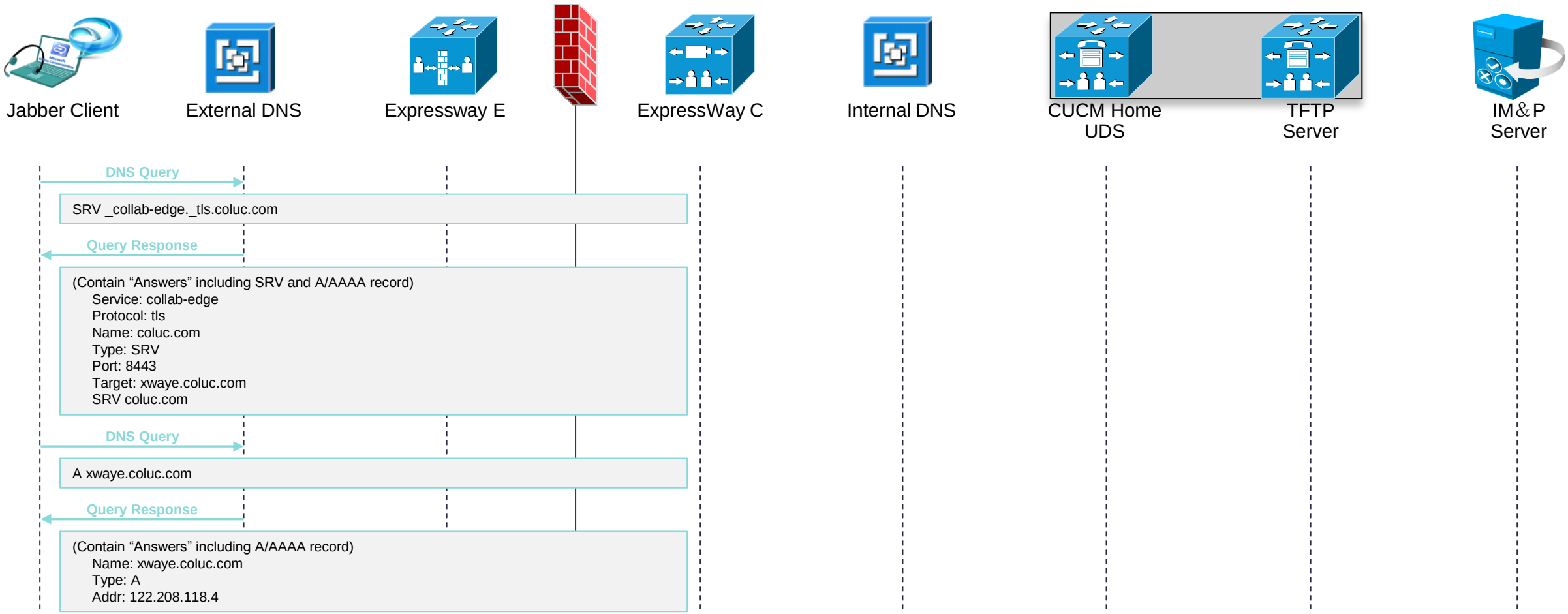
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



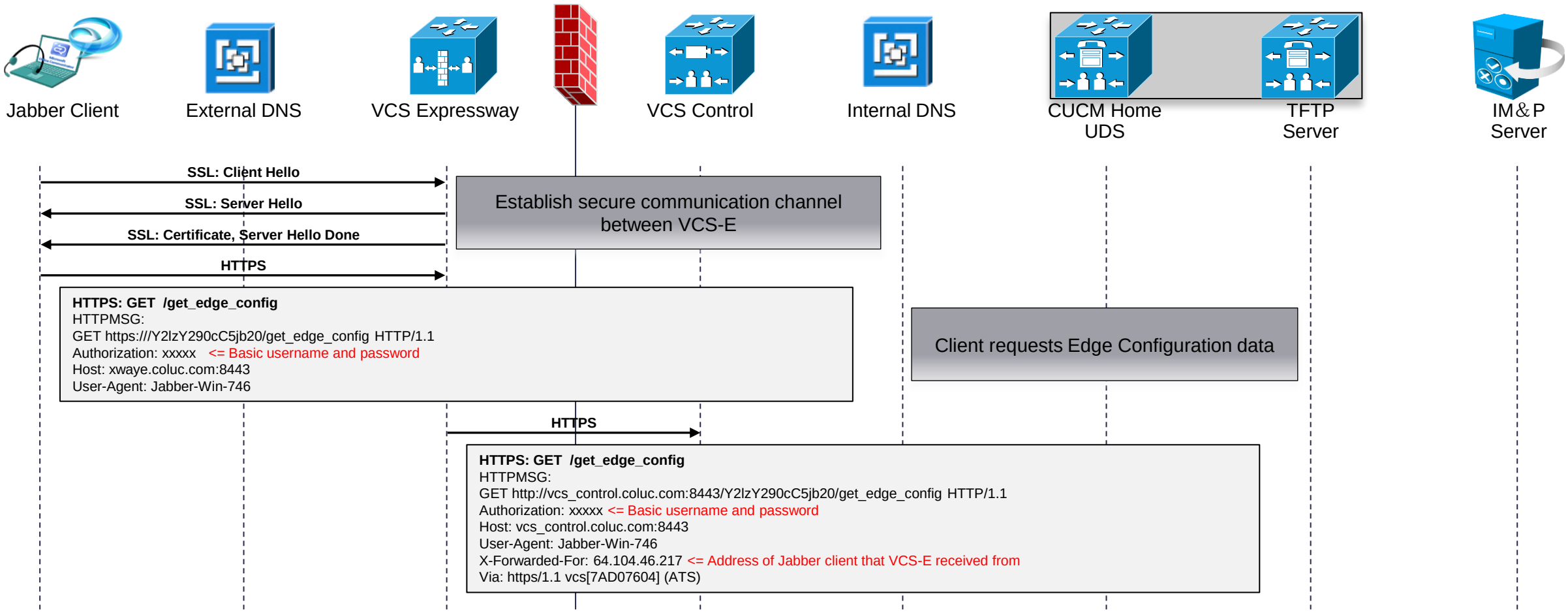
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



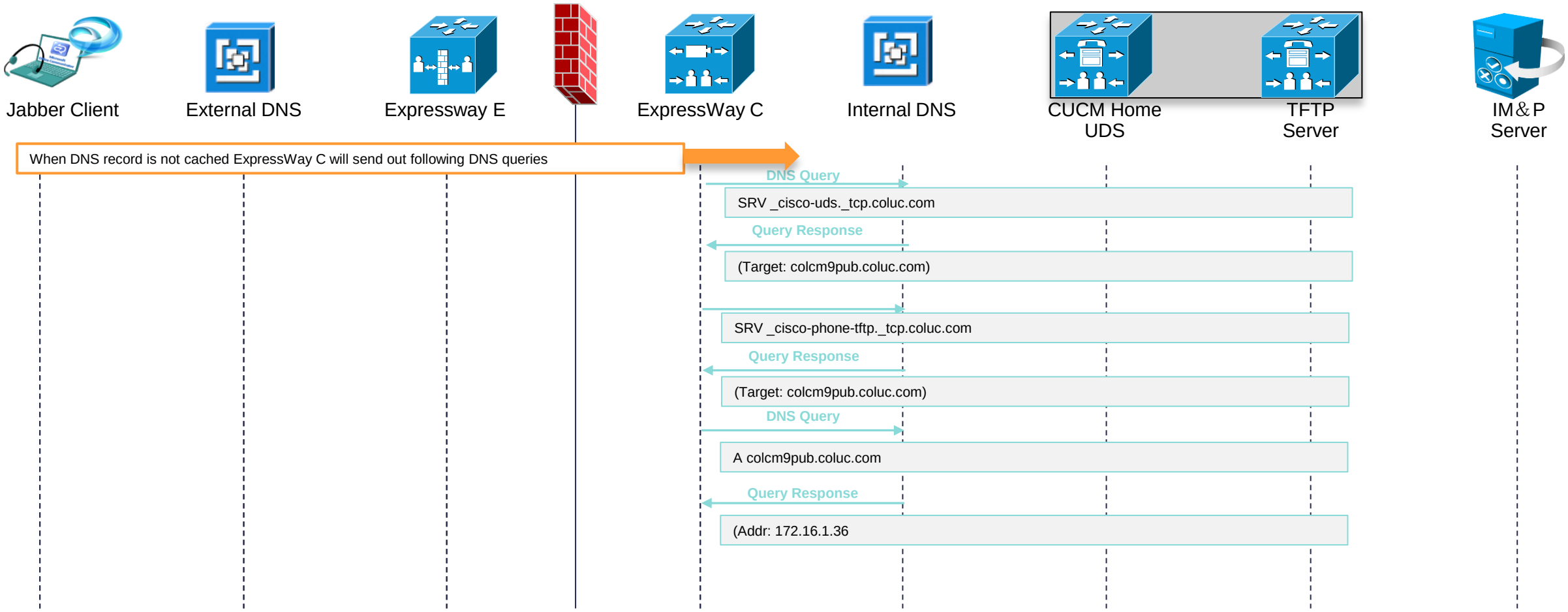
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



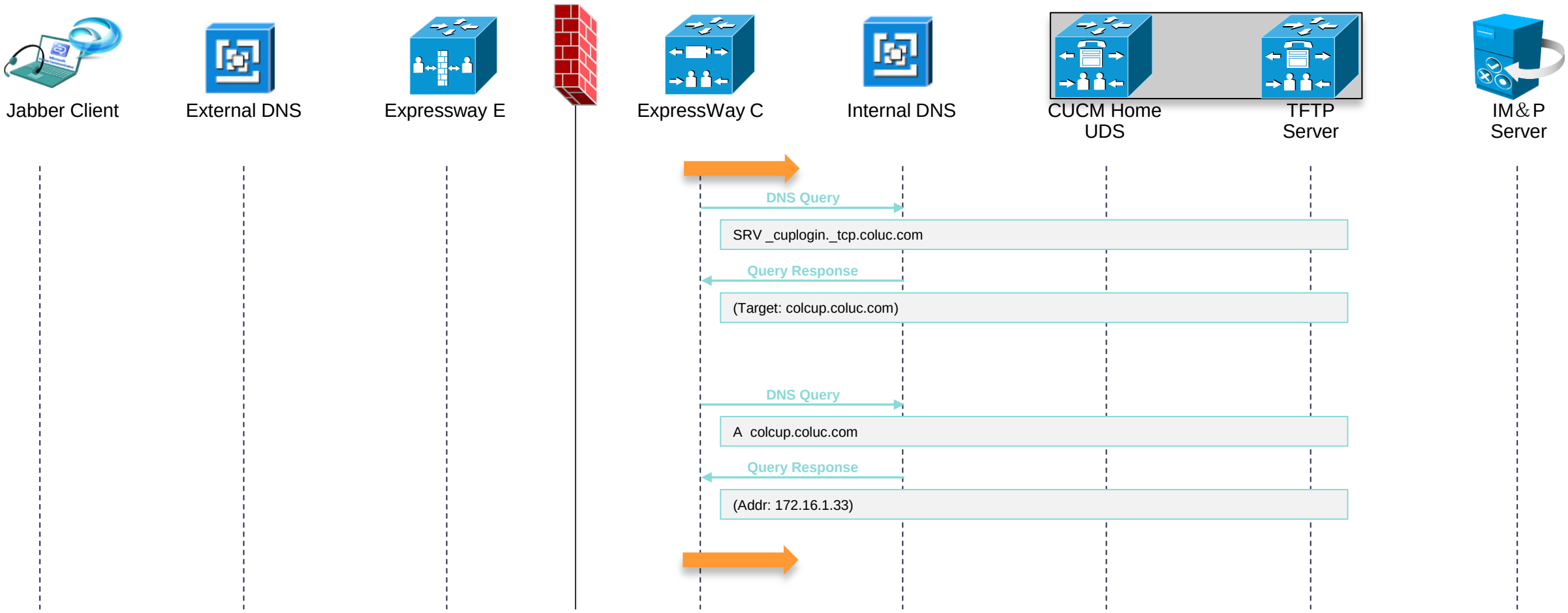
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



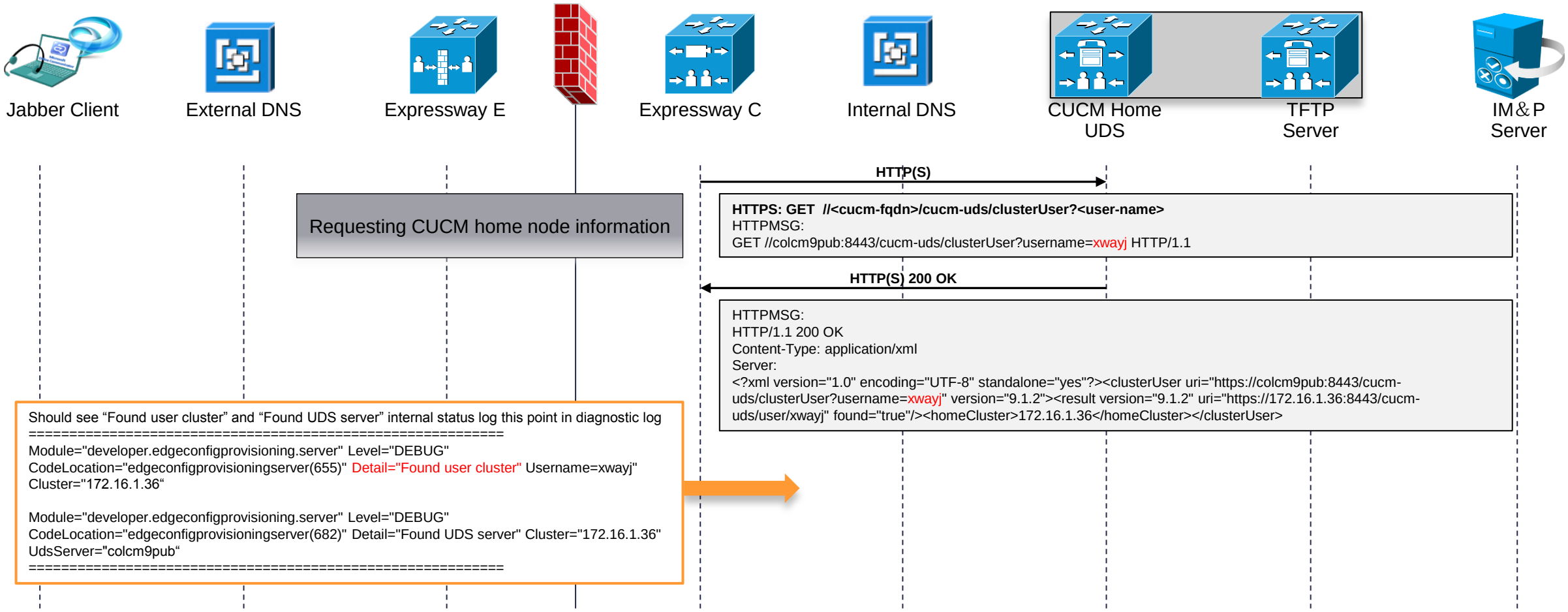
Mobile and Remote Access
– Jabber client connect through MRA

- Register Jabber client on UCM via MRA



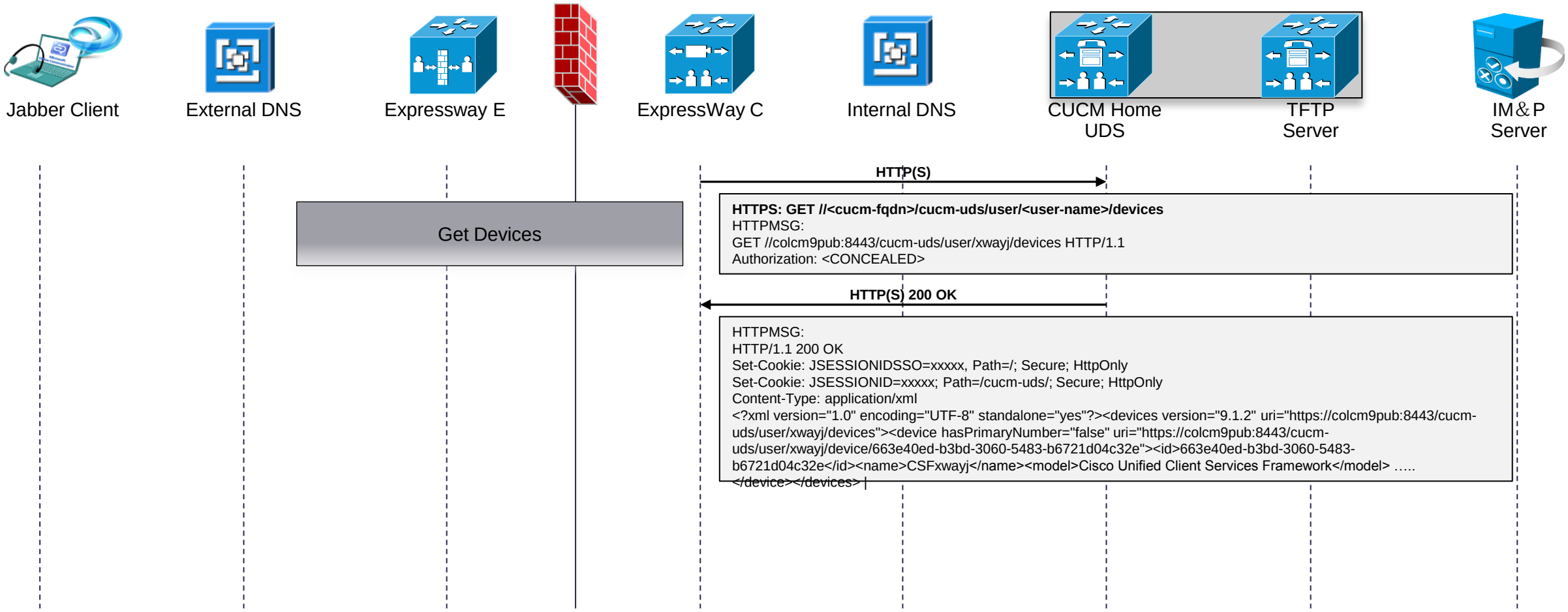
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



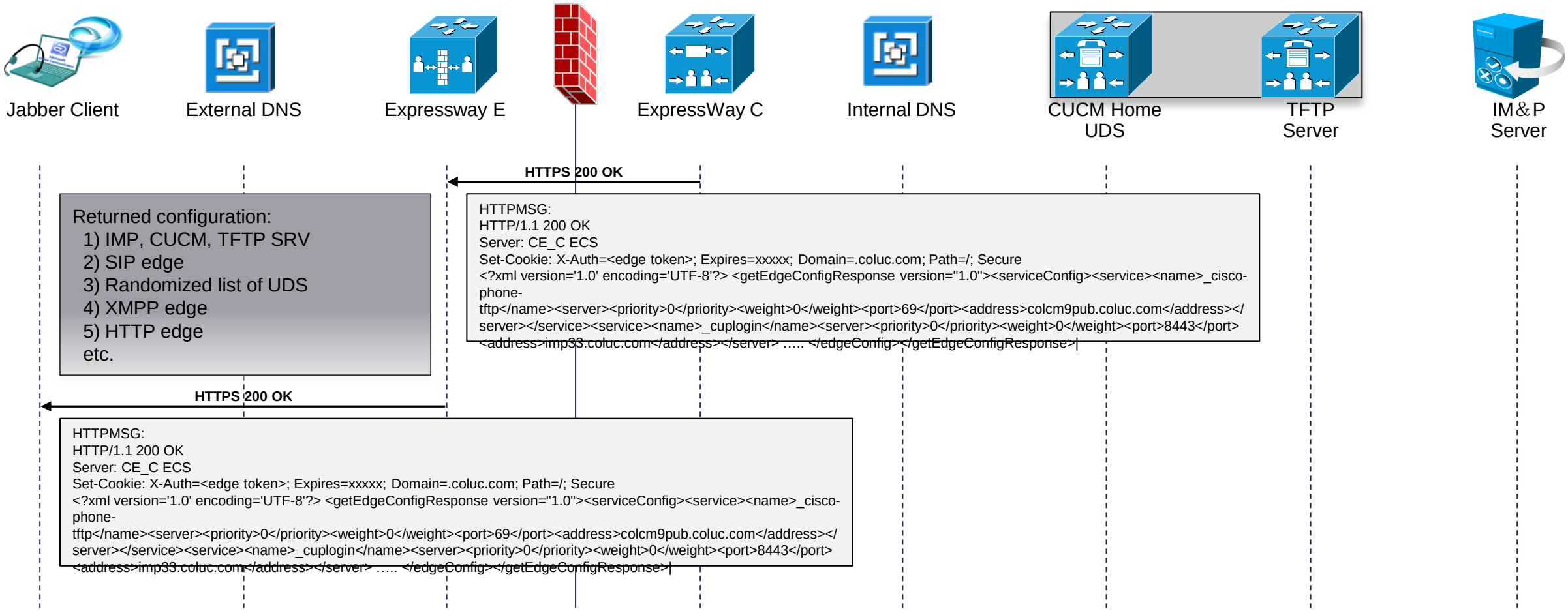
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



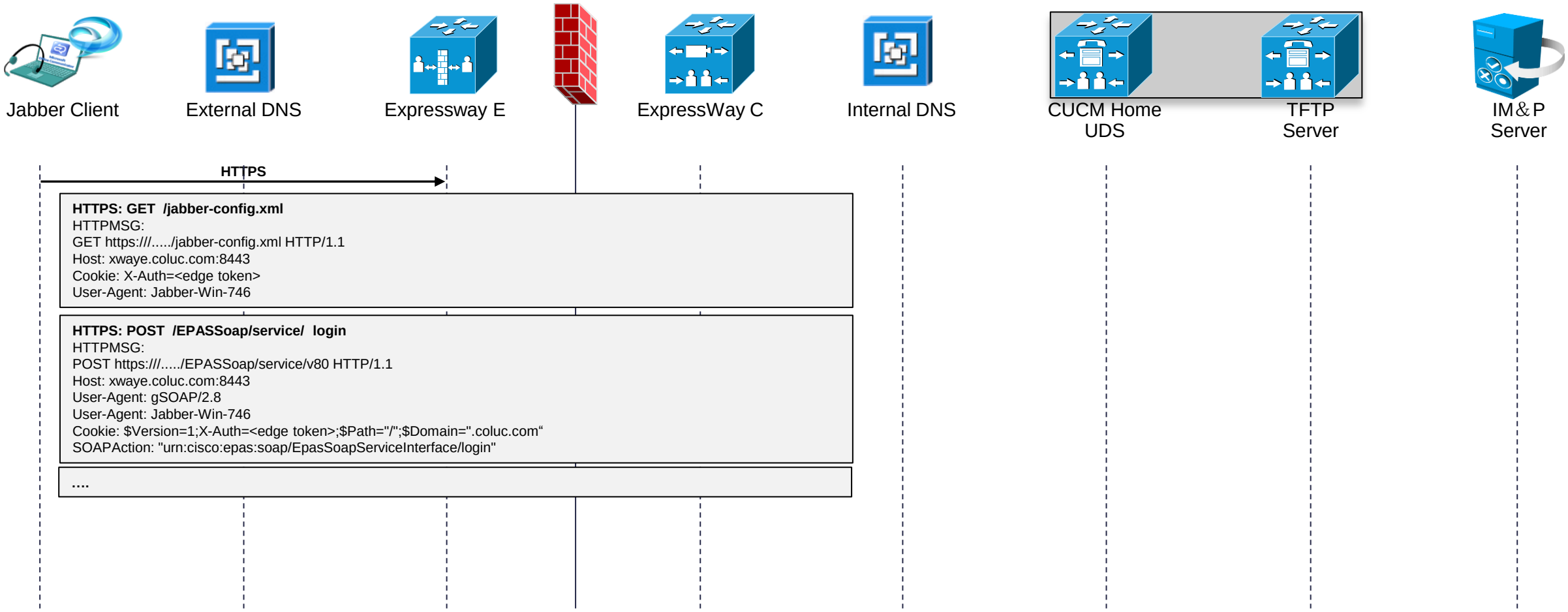
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



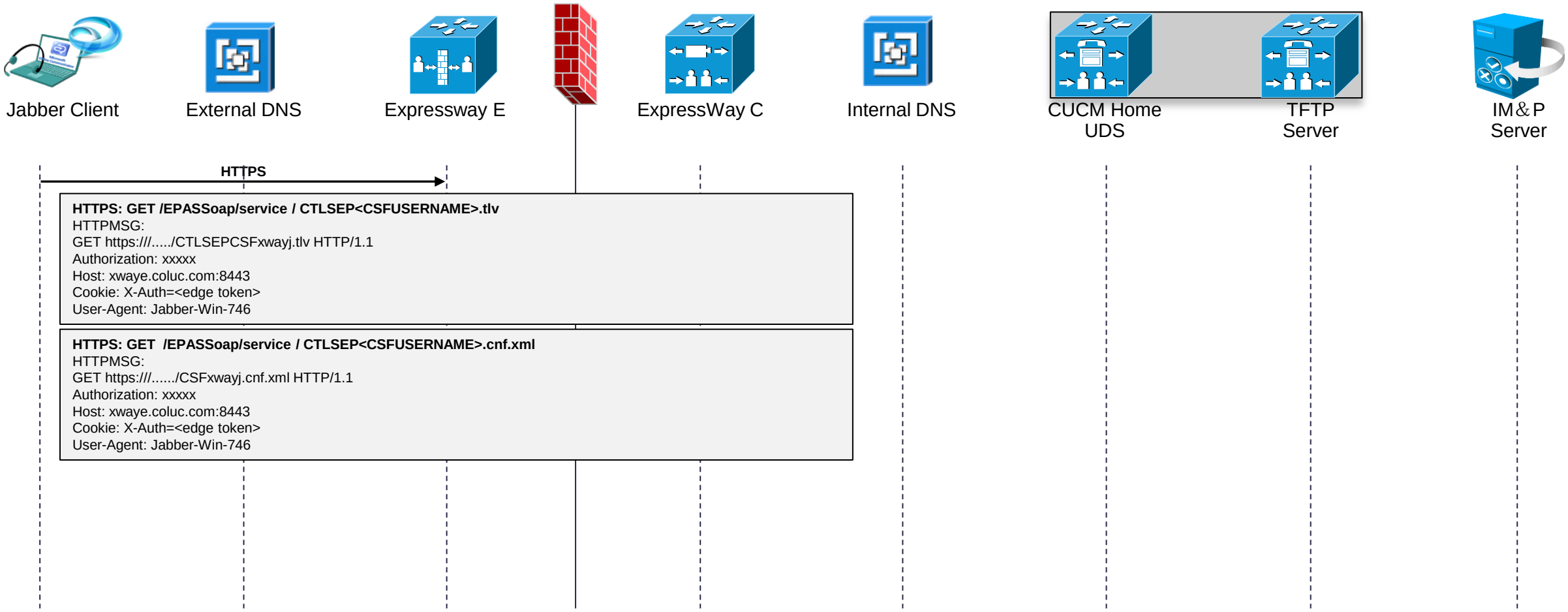
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



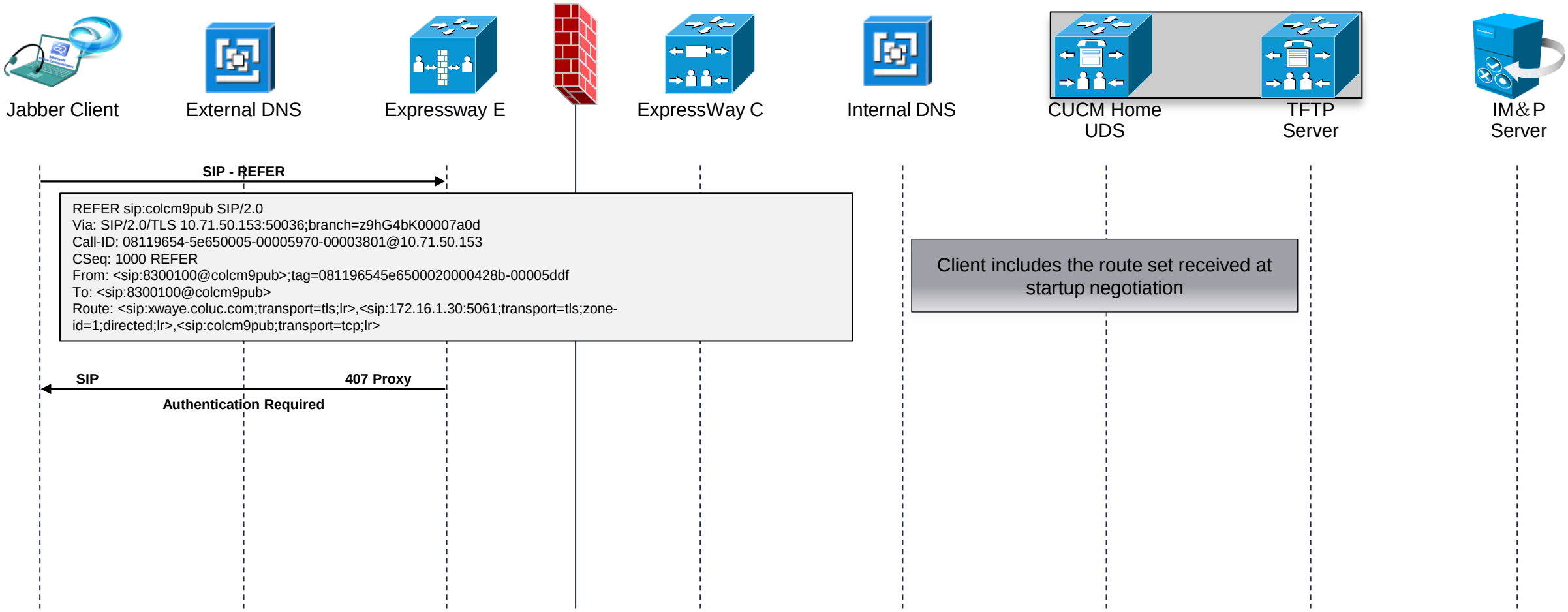
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



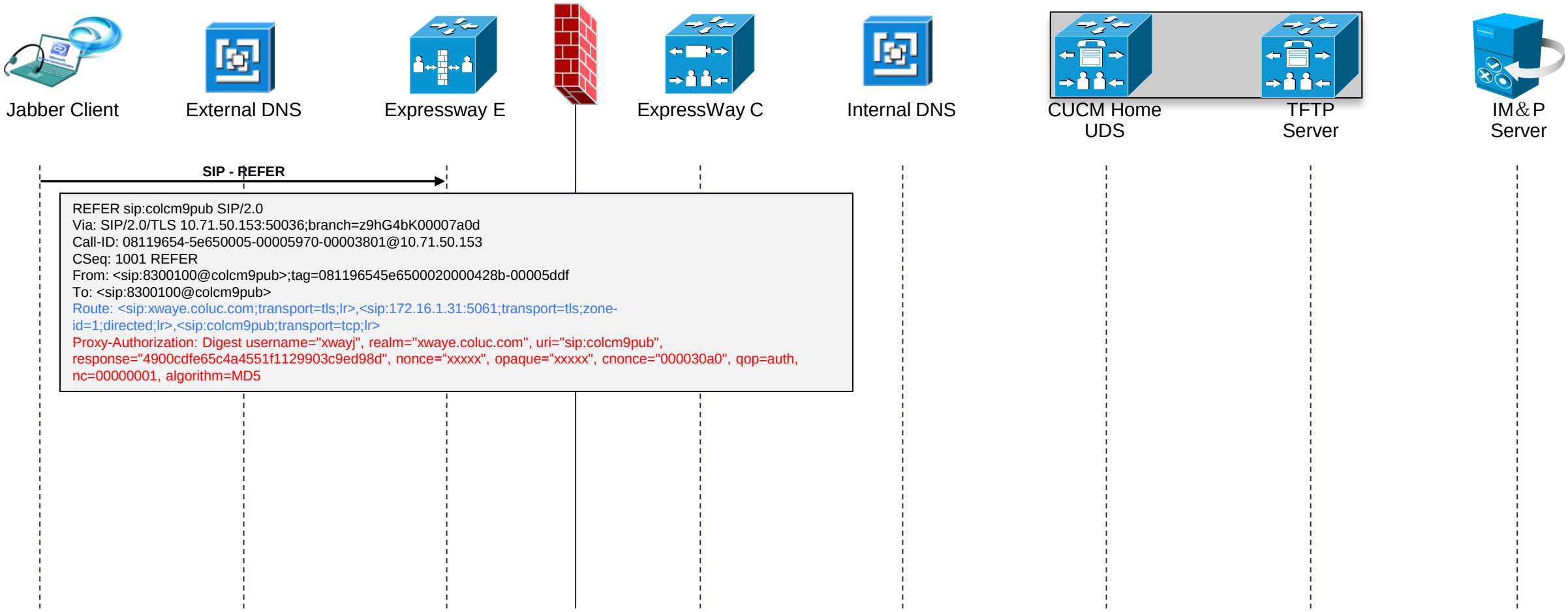
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



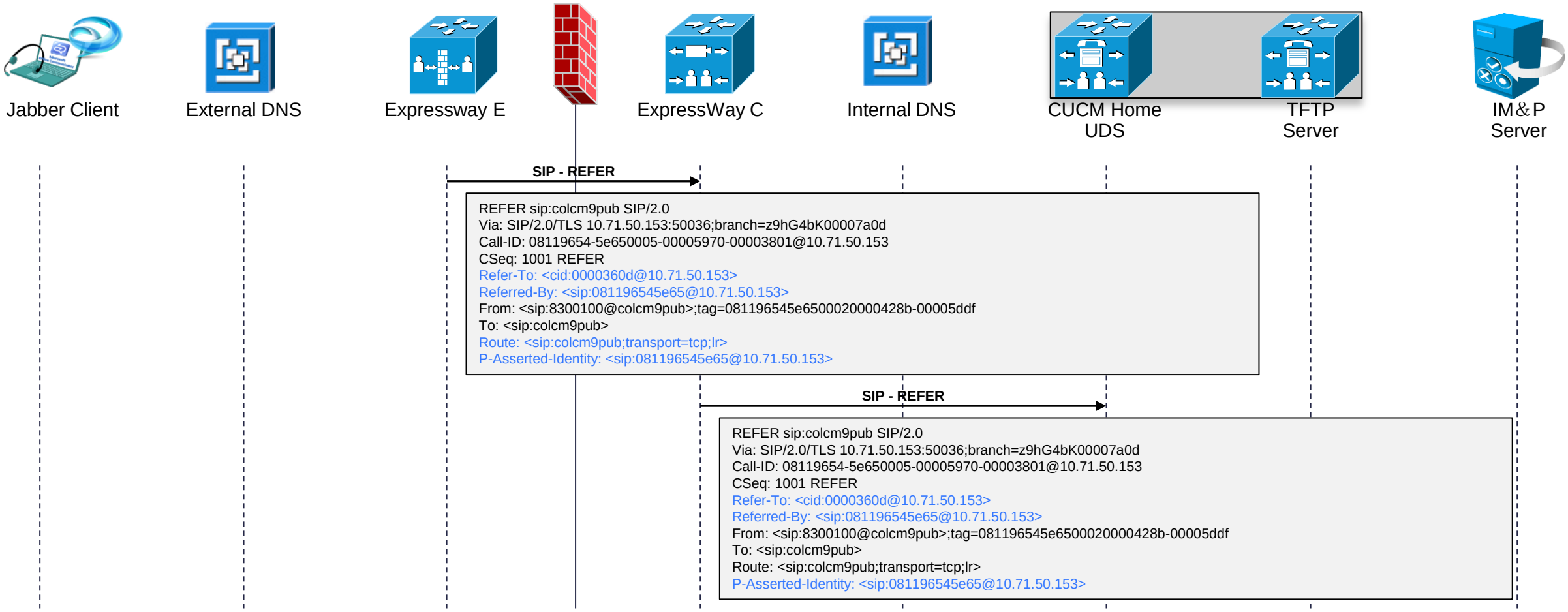
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



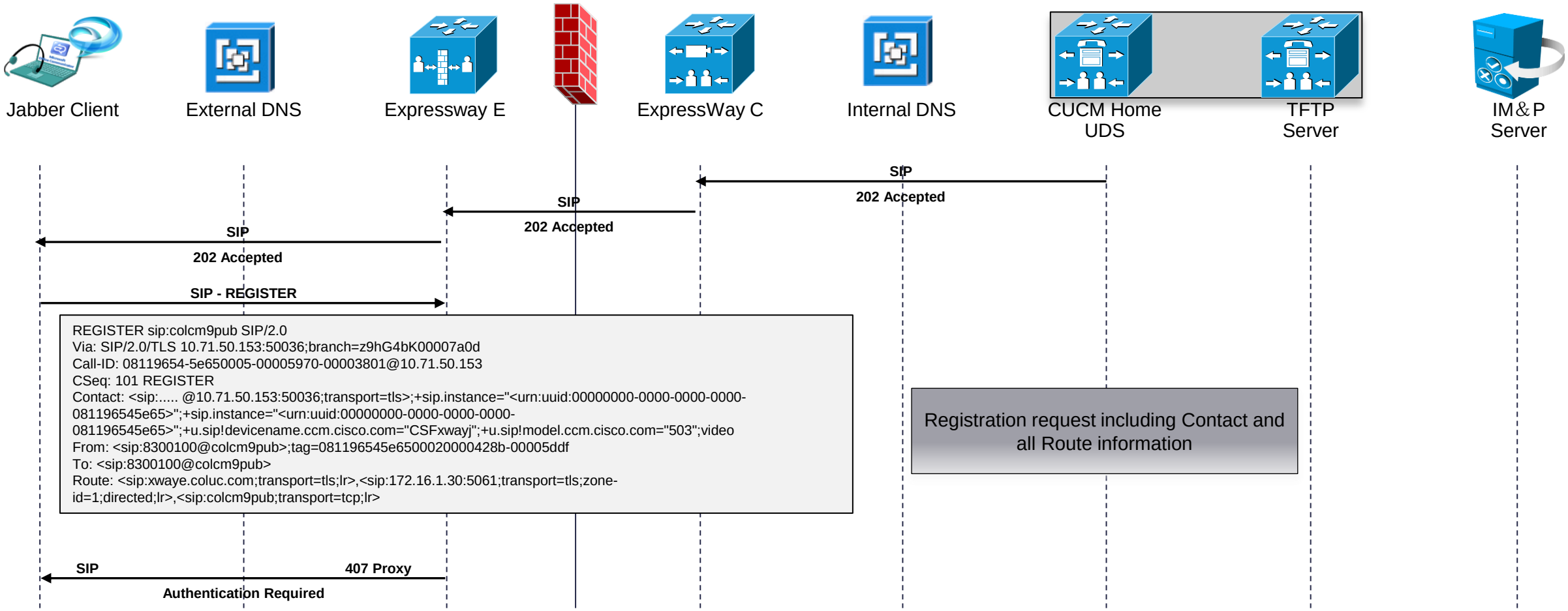
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



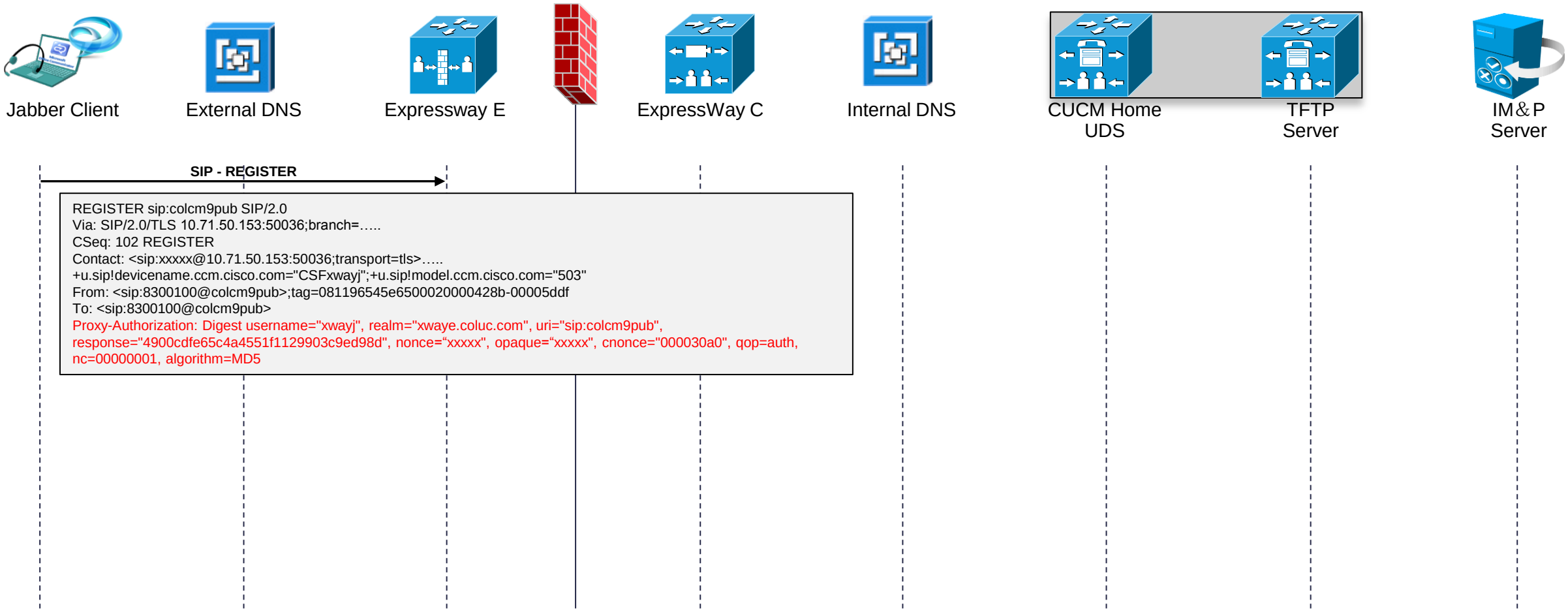
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



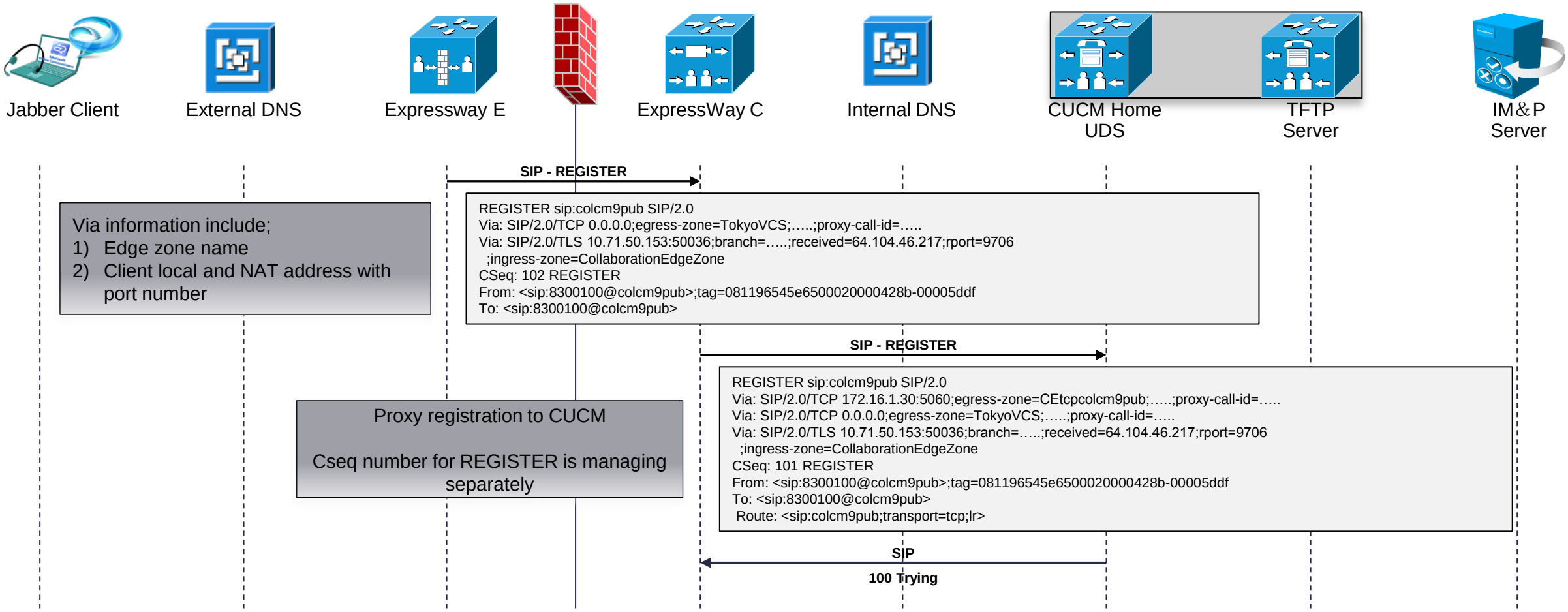
Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



Jabber Registration – Walk Trough

- Register Jabber client on UCM via MRA



References

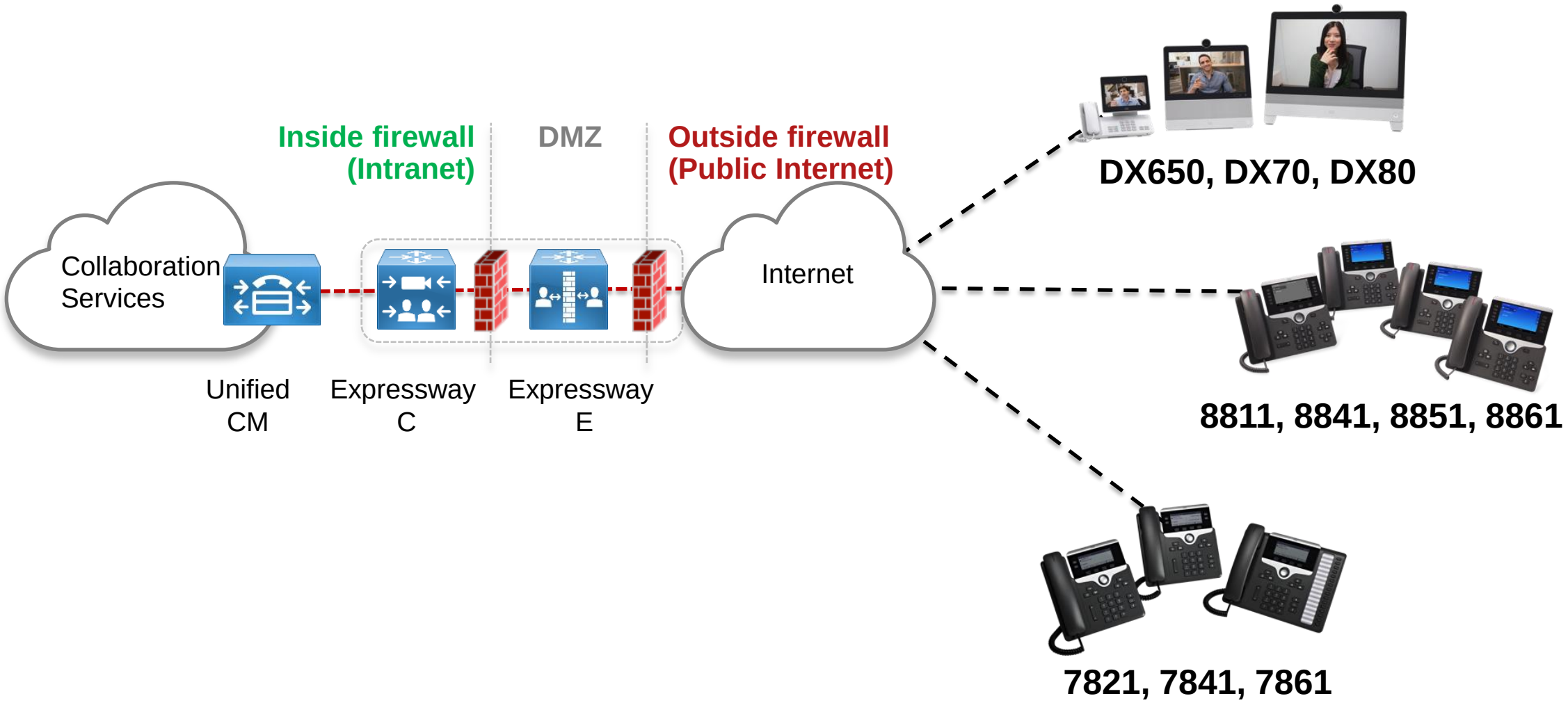
References

- X8.1.1 Mobile and Remote Access deployment guide
  <to be released soon>
- Jabber for Windows 9.7 install/config guide.
  (check chapter on deployment options for more on service discovery)
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/9_7/JABW_BK_C4C679C9_00_cisco-jabber-for-windows-97.html
- Jabber for Windows 9.7 release notes
  Doublecheck what is supported and what not when in edge mode
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/9_7/JABW_BK_CF8F083D_00_cisco-jabber-for-windows-97.html

References

- Base64 encode/decode
  http://www.base64decode.org/

New Endpoint Support



Thank you.